Kim D. Stephens
kstephens@tousley.com
Christopher I. Brain
cbrain@tousley.com
Jason T. Dennett
jdennett@tousley.com
Tousley Brain Stephens PLLC
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992

Interim Lead Plaintiffs' Counsel

Keith S. Dubanevich
kdubanevich@stollberne.com
Yoona Park
ypark@stollberne.com
Stoll Stoll Berne Lokting & Shlachter P.C.
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840

Interim Liaison Plaintiffs' Counsel

[Additional counsel appear on the signature page.]

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

IN RE: PREMERA BLUE CROSS CUSTOMER DATA SECURITY BREACH LITIGATION	Case No. 3:15-md-2633-SI
This Document Relates to All Actions.	**PLAINTIFFS' MOTION FOR CLASS CERTIFICATION AND MEMORANDUM IN SUPPORT OF MOTION** ORAL ARGUMENT REQUESTED **FILED UNDER SEAL**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations

Other Authorities

LOCAL RULE 7.1 CERTIFICATION

Plaintiffs certify that they have conferred in good faith with counsel for defendant in an attempt to resolve the issues presented by this motion but were unable to do so.

MOTION

Pursuant to Federal Rule of Civil Procedure 23, plaintiffs move this Court for an order certifying (1) a nationwide class on a claim under the Washington State Consumer Protection Act, RCW § 19.86.010, *et seq.* ("CPA"); (2) a class of California residents on a claim under the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.* ("CMIA"); (3) a nationwide class on a claim for negligence under Washington law; (4) a nationwide class on a claim for breach of contract; and (5) a nationwide injunctive relief class. Plaintiffs propose that the five classes be defined as follows:

> CPA Class
> All individuals who were, as of March 6, 2015, (i) a current or former member of a Premera Blue Cross health benefit plan or (ii) a current or former non-Premera Blue Cross or Blue Shield member whose health benefit claim was administered by Premera Blue Cross, and (iii) whose Sensitive Information[1] existed in the Premera system.
>
> CMIA Class
> All individuals who were, as of March 6, 2015, (i) a current or former member of a Premera Blue Cross health benefit plan, (ii) were at any time during their membership a resident of California; and (iii) whose medical information, as defined by the California Confidentiality of Medical Information Act, existed in the Premera system.
>
> Negligence Class
> All individuals who were, as of March 6, 2015, (i) a current or former member of a Premera Blue Cross health benefit plan or (ii) a current or former non-Premera Blue Cross or Blue Shield member whose health benefit claim was administered

[1] Sensitive Information consists of confidential information, including name, date of birth, mailing address, telephone number, email address, Social Security number, member identification number, medical claim information, financial information, or any other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

by Premera Blue Cross, and (iii) whose Sensitive Information existed in the Premera system.

Breach of Contract Class
All individuals who were, as of March 6, 2015, (i) a current or former member of a Premera Blue Cross health benefit plan and (ii) whose Sensitive Information existed in the Premera system.

Injunctive Relief Class
All individuals who were, as of March 6, 2015, (i) a current or former member of a Premera Blue Cross health benefit plan or (ii) a current or former non-Premera Blue Cross or Blue Shield member whose health benefit claim was administered by Premera Blue Cross, and (iii) whose Sensitive Information existed in the Premera system on March 6, 2015 and currently exists in the Premera system.

Plaintiffs further request that this Court appoint Kim Stephens of Tousley Brain Stephens LLC as Class Counsel; James Pizzirusso of Hausfeld LLP, Tina Wolfson of Ahdoot & Wolfson, and Karen Hanson Riebel of Lockridge Grindal & Nauen PLLP to the Executive Committee; and Keith Dubanevich of Stoll Berne as Liaison Counsel, pursuant to Federal Rule of Civil Procedure 23(g). Plaintiffs further seek an order appointing plaintiffs April Allred, Elizabeth Black, Ralph Christopherson, Barbara Lynch, Sharif Ailey, Catherine Bushman, Krishnendu Chakraborty, Maduchdanda Chakraborty, Eric Forseter, Mary Fuerst, Ross Imbler, Kevin Smith, and Debbie Hansen-Bosse (collectively, "Plaintiffs") as class representatives.[2]

[2] Plaintiffs April Allred, Elizabeth Black, Ralph Christopherson, and Barbara Lynch seek to represent the proposed CPA, Negligence, and Injunctive Relief Classes. Plaintiffs Sharif Ailey, April Allred, Elizabeth Black, Catherine Bushman, Ralph Christopherson, Krishnendu Chakraborty, Maduchdanda Chakraborty, Eric Forseter, Mary Fuerst, Ross Imbler, Barbara Lynch, Kevin Smith, and Debbie Hansen-Bosse seek to represent the proposed Contract Class. Plaintiff Debbie Hansen-Bosse seeks to represent the proposed CMIA Class.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Millions of Premera and other Blue Cross Blue Shield members entrusted Premera with their most sensitive information, including personally identifying information ("PII") and protected health information ("PHI") (collectively "Sensitive Information"). Premera promised—and was required by HIPAA—to secure this data. But on May 5, 2014, as a result of numerous failures relating to IT security and Premera's knowing and willful neglect of its data security systems, hackers exploited well-known flaws to enter Premera's computer network, where they roamed through Premera's servers undetected for over eight months, and accessed and exfiltrated troves of valuable information about Premera's members.

Sensitive Information is extremely valuable, especially on the black market, making medical insurance companies prime targets for malicious actors. This was common knowledge within the industry (and at Premera) prior to the breach; Premera's external and internal auditors, and even its information technology security teams, warned that Premera was at risk of being hacked.

Despite this knowledge—and the legal and contractual obligations Premera owed to plan members and beneficiaries—Premera maintained financially, technologically, and institutionally inadequate data security measures. Premera failed to allocate sufficient financial and human resources to security, failed to implement critical security protections, and failed to properly configure or monitor existing security programs in the face of numerous requests to do so by its own auditors. These failures were compounded by a dysfunctional corporate structure that led to internal confusion over who was responsible for overseeing security obligations and remediating vulnerabilities. This dysfunction permeated all ranks of Premera's security teams, which

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

developed a culture of denial, even going so far as to lie to internal auditors about the existence of flaws.

The repercussions of Premera's numerous security deficiencies finally came to a head on May 5, 2014, when a Premera employee opened a phishing email that allowed hackers to access and systematically infiltrate Premera's entire network—including databases where Premera stored customers' Sensitive Information. These hackers had more than eight months to take what they wanted from Premera's systems and clean up their tracks to avoid detection before they were discovered. All the while, Premera failed to implement the very safeguards it promised it had to alert Premera to hacking and exfiltration attempts, and failed to monitor those safeguards it did have. In fact, Premera itself never discovered the hackers (its intrusion detection system never having been properly set up or even checked). Rather, Premera first learned about the breach in January 2015 from Mandiant, a third-party forensic investigator Premera hired to analyze a *different* malware infection.

Mandiant's investigation determined that a known hacking group (that had targeted and extracted data from similar entities) was responsible for the breach, and discovered fragments of RAR files, which are created by compression software commonly used by hackers to shrink files to a manageable size before exfiltration. These files were created in the middle of the night, at the same time that the hackers used Premera user IDs to access compromised computers. Premera employees did not create these files, nor are there any automated systems at Premera that would have created them. Mandiant's initial conclusion that the files were evidence of likely data exfiltration was confirmed by another independent cybersecurity investigator, CrowdStrike, who prepared a report for states investigating the Premera data breach. Only after Premera's

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

counsel assumed control over Mandiant's investigation did Mandiant water down its conclusions to claim that there was no proof of exfiltration.

As soon as Premera notified the public of the breach of its data—two months *after* it was discovered and ten months after it began—Premera began to receive calls from consumers and its own employees reporting identity theft and medical fraud. Notably, many of these reports were specifically related to medical and prescription-related fraud from the types of information that would only have been found in Premera's records. Premera ignored those reports, instead choosing to stick its head in the sand and parrot its self-serving, attorney-directed mantra that there was no evidence of data exfiltration. And although Premera engaged in belated remediation attempts to correct its security deficiencies, Premera has *still* not taken the steps necessary to minimize the risk of further exposure.

To prosecute the harms Premera's customers collectively suffered at its hands, Plaintiffs seek to certify five classes of individuals under 23(b)(3) and (b)(2). Alternatively, Plaintiffs seek to certify state subclasses or an issues class under 23(c)(4). As discussed below, the proposed Classes meet all the requirements of Federal Rule of Civil Procedure 23. Accordingly, Plaintiffs respectfully request that this Court certify the classes as identified above.

II. LEGAL STANDARD

Where, as here, plaintiffs seek class certification for money damages, they must affirmatively prove six prerequisites:

> (1) Numerosity. Class certification is only appropriate if it is not practical to join all potential claimants in one litigation. Fed. R. Civ. P. 23(a)(1).
>
> (2) Commonality. At least one legal or factual question must be common to every member of the class. Fed. R. Civ. P. 23(a)(2).
>
> (3) Typicality. The named plaintiffs must have the same type of claim as other class members. Fed. R. Civ. P. 23(a)(3).

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

(4) Adequacy. The named plaintiffs and their counsel must represent the interests of absent class members. Fed. R. Civ. P. 23(a)(4).

(5) Predominance. Legal and factual issues that can be resolved on a classwide basis must be more important than those that could only be resolved on an individual basis. Fed. R. Civ. P. 23(b)(3).

(6) Superiority. A class action must be superior to many individual lawsuits. Fed. R. Civ. P. 23(b)(3).

See, e.g., Amgen Inc. v. Connecticut Retirement Plans and Trust Funds, 568 U.S. 455, 459 (2013) (articulating standards for class certification); *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 979-80 (9th Cir. 2011).

Plaintiffs in this case also seek certification of an injunctive relief class. For certification of such a claim, Plaintiffs need only show the first four elements listed above—*i.e.*, numerosity, commonality, typicality, and adequacy—as well as that a party has "acted or refused to act on grounds that apply generally to the class." Fed. R. Civ. P. 23(b)(2).

III. FACTUAL BACKGROUND

The common evidence produced in discovery thus far is overwhelming and shows that common fact issues predominate. This evidence will be sufficient for a jury to determine, in a unitary trial and on a classwide basis, Premera's liability, harm to the class, and damages. Plaintiffs, who have taken over 15 party depositions, three third-party depositions, and reviewed tens of thousands of documents, provide an overview of the evidence obtained to date below.

A. Premera Obtains Valuable Sensitive Information in Exchange for Providing Health Insurance Benefits and Claims Administration

i. Premera adjusts and pays claims for individuals across the United States.

Premera is one of the largest health insurers in the Pacific Northwest, operating from its headquarters in Mountlake Terrace, WA. Answer to First Am. Consolidated Class Action Compl., ECF No. 98 ("Answer"), ¶¶ 2, 134. Premera provides health benefit policies and plans

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

for numerous companies headquartered in Washington, Oregon, and Alaska that cover employees working in all 50 states and U.S. territories. Declaration of Yoona Park, Ex. 1 (Kemp) at 14:3-8, 17:5-18:4[3]. Premera is also a member of a network of Blue Cross Blue Shield ("BCBS") companies that share provider networks; this Blue Card Program allows Premera insureds to utilize the provider networks of other local Blue companies and for non-Premera BCBS-insureds ("Blue Members") to take advantage of the provider networks Premera has established in Washington and Alaska. *Id.* at 14:9-16:4, 18:19-21:15, 22:8-24:25. Under this program, Premera administers the claims of both in-state and out-of-state BCBS insureds and administers the benefits for all in-state and out-of-state Premera insureds. *Id*.

In order to provide claims administration and health benefits, Premera requires enrollees and their dependents, and "Blue members" to provide Sensitive Information, including persistent identifiers such as names, dates of birth, social security numbers, member identification numbers, medical claims information, mailing addresses, telephone numbers, and healthcare information, and transient identifiers such as financial information (including credit card payment data). *Id.* at 18:19-20:6; Declaration of James Van Dyke ("Van Dyke Decl.") at ¶ 14. As an insurer, Premera is obligated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to adopt administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of the Sensitive Information it receives. 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312. Premera's customers expect that Premera will not only comply with its HIPAA obligations, but also adhere to industry standards and contractual obligations regarding data security to ensure the confidentiality of their valuable PII. *See, e.g.*,

[3] Unless otherwise stated, all references to exhibits herein shall refer to the corresponding exhibits attached to the Declaration of Yoona Park and will be cited as "Ex. ___".

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Ex. 2; Ex. 3 (Imbler) at 70:15-71:25; Ex. 4 (Chakraborty) at 33:24-34:14. Indeed, Premera sent each of its members a Notice of Privacy Practices in which it "committed to maintaining the confidentiality of your medical and financial information" and promised that Premera would "take steps to secure [its] buildings and electronic systems from unauthorized access." Ex. 5 at PBC_TAR00149218; Ex. 6 at PBC_TAR00026296; Ex. 7. Premera failed to fulfill its promise when, as a result of its deficient security practices, hackers breached Premera's network and gained access to its data—including Sensitive Information —and remained undetected for eight months.

ii. Sensitive Information is extremely valuable on the black market.

There is an aphorism that criminals rob banks "because that's where the money is." Today, the money is also in data. Sensitive Information is extremely valuable in part because criminals can use it to steal money and prescription drugs by filing false tax returns, opening fraudulent credit accounts, and creating false medical IDs. *See, e.g.*, Van Dyke Decl. at ¶ 22; Declaration of Dr. Coleman D. Bazelon ("Bazelon Decl.") at ¶ 22, 24, 32-34. Premera acknowledges the high value of Sensitive Information on its system, estimating that social security numbers alone are sometimes sold for as much as $5, whereas healthcare data can be sold for $70 and upwards. Ex. 8 at PBC_TAR00911381; *see also* Van Dyke Decl. at ¶ 44-48 (explaining the ranges of values for PII and PHI). As a basic economic matter, there is no serious dispute that a person's Sensitive Information has significant monetary value. Bazelon Decl. at ¶ 37.

iii. Premera knew that it was a target for hackers; the US government and others issued warnings to Premera about its data security vulnerability.

Due to the valuable nature of Sensitive Information, health insurance companies have long been targets of hackers and other malicious actors. In 2012 and 2013, Verizon Business, a

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

leading data breach industry consultant, reported on the prevalence of hacking and malware threats, with breaches in the Health Care and Social Assistance industries making up over 7% of total breaches worldwide. Ex. 9 at 11; *see also* Ex. 10.

The federal government also issued industry-wide and Premera-specific warnings regarding data security. For example, on April 8, 2014, just a month before Premera's systems were hacked, the Federal Bureau of Investigation's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that the health care industry was a particularly susceptible target for cyber attacks. Ex. 11. The Notification specifically warned that "[t]he health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely." *Id*. Moreover, the U.S. Office of Personnel Management ("OPM") found numerous security flaws during a routine audit of Premera's systems, which it reported to Premera a few weeks before the breach. The report noted "several areas of concern related to Premera's network security controls" including that "patches are not being implemented in a timely manner," "a methodology is not in place to ensure that unsupported or out-of-date software is not utilized," and a vulnerability scan identified "insecure server configurations." Ex. 12 at PBC_TAR00010427.

By the time of the May 2014 data breach, Premera knew that it was at particular risk from malicious actors seeking to gain access to its systems and confidential customer data. This was common knowledge within the industry, including within Premera's IT department. Ex. 13 (Christian) at 121:4-122:10. In 2013, Premera's training materials discussed the risk of social engineering attacks, including phishing attempts, by someone "pretending to be IT and having the user perform malicious actions or hand over credentials." Ex. 14 at PBC00016758. And at the same time the hackers were infiltrating the system and roaming unrestricted in Premera's

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

database, Premera's own security team made presentations about the known risk of theft of customer data through third-party breaches. Ex. 13 (Christian) at 19:12-22:24; Ex. 15; *see also* Ex. 16.

B. Despite Repeated Warnings About its Security Vulnerabilities, Premera Failed to Implement Adequate Security Mechanisms to Safeguard Customer Sensitive Information

Despite Premera's knowledge that the value of the Sensitive Information on its system made it particularly attractive to potential hackers, and despite Premera's legal obligations under HIPAA, state law, and its contracts, Premera wholly failed to implement necessary security protocols and mechanisms to ensure the security of the confidential customer data within its care. This common and predominating evidence of Premera's failures directly led to the breach in this case.

i. Premera failed to allocate sufficient and adequate resources to data security.

In the years leading up to the breach, Premera continuously prioritized its business interests over the security of the sensitive customer data in its care. Premera spent just 1-1.5% of its information technology budget on data security, significantly less than the industry average of over 4.5% during this time period. Ex. 17 at PBC00149883. Management often denied requests for additional security funding, even for the highest risk vulnerabilities. Ex. 18 (Robinson) at 30:18-35:16, 50:4-13, 118:15-120:17; Ex. 16. Premera even shortchanged security funding requests associated with HIPAA compliance. For example, in September 2013, Eric Robinson, senior manager of Premera's Information Security Department, put together an analysis and remediation plan to meet certain HIPAA requirements; he asked for over $1.5 million to accomplish this task, but Premera provided only a few hundred thousand. Ex. 18 (Robinson) at 13:14-25, 80:19-83:5, 84:1-85:6; Ex. 19; Ex. 20 (Voges) at 67:5-68:7. Premera's security team

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

repeatedly complained that they did not have enough employees to complete assigned tasks. Ex. 21 (Twitchell) at 226:5-18; Ex. 18 (Robinson) at 114:1-115:5, 137:20-138:16, 158:8-23, 162:9-163:1, 165:19-166:11, 227:4-20, 241:21-243:11; Ex. 22; Ex. 23; Ex. 24; Ex. 1 (Kemp) at 123:11-125:6; Ex. 25; Ex. 13 (Christian) at 185:19-187:3; Ex. 20 (Voges) at 30:24-31:6; Ex. 26 at PBC00190205. The need for additional resources to meet Premera's security obligations left one employee feeling like he was on a "sinking ship." Ex. 18 (Robinson) at 162:9-23. And IT security employees even acknowledged that IT security "won't get what we want until we have a breach." Ex. 24 at PBC_TAR0041817.

The issues resulting from the financial and human resource constraints were further compounded by the fact that senior IT executives did not have sufficient background or knowledge to comprehend fully the risks and preventative measures necessary to protect sensitive data within Premera's possession. Further, IT executives had significant conflicts of interest with their business-side obligations. For example, in January 2014, Premera promoted Kacey Kemp to Executive Vice President of Information Technology, giving her accountability over that sector, despite the fact that her background was in operations, not IT. Ex. 1 (Kemp) at 10:8-12:1. Predictably, the security team was frustrated by Kemp's lack of IT knowledge. Ex. 20 (Voges) at 175:20-176:13, 177:14-21. In her role as EVP of IT, and in her interim role as default CIO (after the previous CIO was fired for performance issues), Kemp was not provided with information regarding security risks and deficiencies necessary for her to perform her job—and even when she was provided with information, she had only rudimentary knowledge of technical issues, which prevented her from ensuring that proper security protocols were followed. Ex. 1 (Kemp) at 37:16-38:4, 67:18-71:13, 78:12-79:5, 84:21-85:12, 91:2-95:22, 101:24-103:23, 106:3-113:5, 122:5-123:9; 126:18-127:10, 156:4-157:13, 166:6-21; Ex. 20 (Voges) at 177:14-21; Ex.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

27 ("[Kemp] commented that she's having trouble understanding what she needs to worry about. It might be good to help give [Kemp] a little decoder ring.").

Likewise, Premera's corporate structure had inherent conflicts of interests. For over a decade, the information security team and infrastructure team reported to the same vice president. This corporate structuring meant that the same person was forced to choose between business functionality and security interests when the two conflicted, and there was "the potential that business pressures could sway the decision away from security far too easily." Ex. 28 (Vergeront) at 173:1-178:12, 181:6-182:3; Ex. 29; Ex. 18 (Robinson) at 234:13-235:12; Ex. 20 (Voges) at 137:4-138:14. Despite the fact that Premera identified this conflict as a deficiency at least as early as 2002, the reporting structure was left in place until 2015. In fact, throughout the relevant time period, Premera repeatedly failed to remediate critical security deficiencies in deference to its business considerations and financial bottom line. Ex. 18 (Robinson) at 13:14-25, 80:19-83:5, 84:1-85:6.

ii. Premera's internal and external auditors repeatedly found multiple, critical flaws in Premera's data security that Premera failed to remediate.

a. Internal and external audits in the years preceding the breach revealed critical deficiencies that Premera did not remediate.

Premera regularly engaged third-party consultants to assess the state of its data security and conducted internal audits to identify any deficiencies in its security protocols, software, and processes. The critical problem was that this was all window dressing; Premera repeatedly ignored the results and failed to remediate the numerous critical deficiencies that outside and internal consultants routinely and repeatedly identified.

The external audits were characterized by *repeat* deficiency findings in key security areas. For example, in 2011, Premera hired Verizon Business Solutions to perform a series of

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

tests and investigations of Premera's networks to identify security risks. Verizon prepared four reports identifying numerous critical and high risks, including on issues related to: patching, IDS/IPS[4] monitoring, logging, servers, and employee security awareness. Exs. 30-33; *see* Declaration of Matthew Strebe ("Strebe Decl."), Ex. B(n), (p), (q)[5]. Similarly, in 2012, Accuvant assessed Premera's security and noted critical and high deficiencies with respect to, among other things: social engineering, network segmentation, security policies, log aggregation, patching, IPS, and weak passwords. Ex. 34; *see* Strebe Decl., Ex. B(a). In 2013, Accuvant performed another assessment and again found problems with Premera's security, including network segmentation, patching, social engineering, and passwords. Ex. 35. Coalfire Labs' assessment in 2014 likewise found deficiencies in patching, social engineering and network segmentation. Ex. 36-38; *see* Strebe Decl., Ex. B(g). Premera failed to assign ownership to track and remediate these issues in a timely manner. Exs. 39-41.

Unsurprisingly, Premera's own internal IT security audits reported similar critical deficiencies. Premera employed two information technology auditors who would conduct annual and biennial audits to assess various aspects of IT at Premera, including numerous security issues. Ex. 42 (Klouzal) at 21:7-16; Ex. 28 (Vergeront) at 41:14-42:4. Notably, in 2013 and 2014, Premera conducted IT HIPAA Security audits,[6] which identified persistent "significant deficienc[ies]" and "deficienc[ies]" that were not remediated until after the data breach occurred. Exs. 43-44; Ex. 42 (Klouzal) at 131:22-135:2.

---

[5] Definitions for technical terms, such as IDS monitoring are provided for the Court's convenience in the Declaration of Matthew Strebe at ¶ 48, Exhibit B.

[6] Premera withheld the audit documents, but not their overall conclusion, on privilege grounds.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

b. Premera did not properly configure or monitor its Intrusion Detection System.

An Intrusion Detection System ("IDS") "is a critical tool in the detection of malicious activity." Ex. 41 at PBC00164409; Strebe Decl., Ex. B(n). "It's a set of systems that looks at information being passed throughout Premera. . . to determine if there are any unauthorized accesses or to see if there are attempts [to access and reports. . .] the unwanted or malicious activity to the security organization." Ex. 28 (Vergeront) at 191:13-192:11; Ex. 41. It is a "key tool" that is "essential to detect intruders." Ex. 45 at PBC00042921-922. Premera's IDS suffered from two critical flaws: (1) it was not properly configured to align with industry requirements, and, even if it had been properly configured, (2) it was not being monitored.

As far back as 2011 (and perhaps earlier), external auditors noted that Premera lacked IDS monitoring on critical networks and warned Premera that "an attacker could launch an attack against a system located behind one of these firewalls and gain access to sensitive data." Ex. 31 at PBC00000603. Premera's security engineers acknowledged that a "best practice IDS requires the use of sensors 1) at network gateways 2) at the hosts and 3) throughout the network (See NIST SP800-94)" but that Premera only deployed items "1) and 2) in a limited fashion and 3) not at all." Ex. 46 at PBC_TAR00574670.

But while improvements were made to the IDS, those improvements made little difference because Premera was not actively monitoring IDS on a regular basis. In its 2014 audit, Internal Audit ("IA") determined that IDS monitoring had not been performed since March 2013. Ex. 41 at PBC00164409. IT personnel were aware that IDS was not being monitored, but "lower management, middle management, and upper management" all had different views about whether IDS monitoring was being performed and who was handling it. Ex. 28 (Vergeront) at

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

197:20-198:25, 225:1-13, Ex. 47; Ex. 48; Ex. 49; Ex. 22. IA remarked that IDS was a repeat deficiency—having also been found deficient in 2007 and 2012. Ex. 41.

c. Premera did not block data transfers leaving its network because it failed to properly install, configure, and monitor its Data Loss Prevention system.

Data Loss Prevention ("DLP"), if properly configured, monitors data leaving the environment by email, through firewalls, or by a USB device, and has the capability to block data transfers. Ex. 28 (Vergeront) at 90:4-14, 95:11-25; Ex. 40 at PBC00164456-57; *see* Strebe Decl., Ex. B(j), (dd). Premera utilized Symantec's "Vontu" product for DLP. S*ee* Strebe Decl., Ex. B(dd). Like IDS, Premera's DLP software was never fully implemented, because Premera refused to dedicate sufficient resources to perform the necessary monitoring. Ex. 18 (Robinson) at 114:1-115:5. When operating correctly, DLP flags transactions sending data out of the environment and holds them until someone has an opportunity to review and approve the transfer. *Id*. But due to human resource constraints, Vontu was not blocking transfers at Premera, only recording them. *Id*. Premera destroyed these logs and cannot produce them to Plaintiffs.

Both the 2013 and 2014 audits noted DLP-related deficiencies because of a lack of regular testing and the failure to block unauthorized transfers of Sensitive Information out of Premera's computer systems. Ex. 28 (Vergeront) at 117:22-119:6. In 2013, IA "identified multiple failures of the data loss prevention (DLP) software to block unauthorized PPI transfer via . . . external email accounts. . . . This may result in unauthorized transfer of PPI without the company being aware." Ex. 40 at PBC00164456. In the 2014 audit, IA noted that the Enterprise Risk Management Committee *accepted* this risk, allowing employees to send PII off Premera's network through external email accounts, despite the fact that Premera would not know when this occurred. Ex. 41 at PBC00164410.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

d. Premera did not monitor HIPAA-required data logs.

In addition to the DLP and IDS logs, Premera was also required by law to log and monitor access events to its most critical information; including to databases such as FACETS, where Premera stored its members' Sensitive Information. 45 CFR §164.308(a)(1)(ii)(D); 45 CFR § 164.312(b); *see* Strebe Decl., Ex. B(k). Premera's IT policies reflect this requirement. Ex. 50. Premera was also required under HIPAA to monitor log-in attempts to its systems. 45 C.F.R. § 164.308(a)(5). However, Premera's internal auditors repeatedly warned Premera that its log monitoring practices were deficient and failed to comply with HIPAA requirements. In 2014, IA noted that "log-in monitoring was not being adequately or consistently monitored in accordance with published IT procedures" and designated it a repeat deficiency, in violation of HIPAA requirements. Ex. 41 at PBC00164409. Indeed in 2012, IA identified the same issue, noting that there was "no evidence that IT has developed a logging and monitoring process that would satisfy the HIPAA requirements." Ex. 51 at PBC_TAR00639322; Ex. 42 (Klouzal) at 70:25-74:9.

e. Premera did not properly configure or monitor its log aggregator, Splunk.

In order to monitor its IDS and track the various access logs its programs were supposed to generate, Premera implemented a log aggregator system in late 2013 called Splunk. Ex. 28 (Vergeront) at 211:1-13; *see* Strebe Decl., Ex. B(bb). The primary purpose of Splunk is log analysis. The program assembles and aggregates access log data together into one file that Splunk can analyze and a user can manually monitor. Ex. 28 (Vergeront) at 130:6-132:6. Based upon programmed rules, Splunk can send out alerts for critical findings identified in the aggregated logs. *Id.* Splunk is thus a crucial tool for analyzing Premera's HIPAA-required logs

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

and other data. And Premera relied on Splunk to meet its obligations to monitor and promote awareness of information activity critical to securing its electronic PHI. Ex. 52.

Unfortunately, from 2013 through the time of the breach, Premera failed to properly configure or monitor Splunk. For example, Splunk could have been programmed to alert on key logs related to the protection of electronic Sensitive Information, such as security logs (denied access, escalated access); IDS logs; firewall logs; logon attempts, whether successful or not; account lockouts or suspensions; the addition, deletion or modification of privileges related to system or database access; and even the addition or deletion of the logs themselves. Ex. 28 (Vergeront) at 140:22-144:21. However, Premera did not program even one of these logs in Splunk to send an alert. *Id.* As of December 2014, Premera only programmed Splunk to alert on one data point relating to changes in membership. Ex. 28 (Vergeront) at 135:15-140:6; Ex. 52; Ex. 18 (Robinson) at 160:20-162:8. IA was critical of this deficiency, noting that "good contractor dollars should have been put in place" to program Splunk with simple alerts. Ex. 52 at PBC_TAR00573541. Instead, Premera's configuration and implementation of Splunk (like much of its IT security) was haphazard, ineffective, and inadequately funded. *Id.*

From at least April through December 2014, no one was assigned to review Splunk logs and no one regularly monitored this critical log data. Ex. 53 at PBC_TAR00011128-29. Premera did not spend the money on automated software to review Splunk logs, and denied employee requests for this software, Ex. 42 (Klouzal) at 64:17-65:14; Ex. 18 (Robinson) at 160:20-162:8. Inexplicably, when the Network team requested access credentials to review Splunk logs, their request was denied. Ex. 54. Though the monitoring deficiencies are well-documented, the issue was not escalated properly, as the Chief Information Officer, William Voges, testified he found "it difficult to believe that nobody was monitoring it." Ex. 20 (Voges) at 63:11-25.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

f. Premera poorly maintained internal firewalls.

A firewall is a device "that sits on the outer edge of a computing environment" and "is specifically set up to either allow or disallow access for people trying to get through that area." Ex. 28 (Vergeront) at 75:9-15; *see* Strebe Decl., Ex. B(m). In 2013, IA criticized Premera for allowing too many people permission to make changes to its firewalls. Ex. 28 (Vergeront) at 75:16-22; Ex. 18 (Robinson) at 62:11-63:10. Additionally, firewall rule changes were "rarely reviewed by Information Security Engineering to ensure they meet security requirements" and "many changes did not contain adequate documentation." Ex. 40 at PBC00164455-56; *see also* Ex. 18 (Robinson) at 112:21-113:25; Ex. 55 at PBC_TAR00572194. Moreover, Premera failed to periodically review its firewall rules, resulting in rules that were out of date or unused. Ex. 40; Ex. 42 (Klouzal) at 41:6-42:20; Ex. 55 at PBC_TAR00572194. One employee, Eric Robinson, prepared a network and firewall strategy for Premera in 2013, which included a recommendation for adding additional "firewalls and IDS everywhere." Ex. 18 (Robinson) at 206:10-208:9; Ex. 56. While Robinson brought his proposal to the then-current CIO, Kirstin Simonitsch, and other senior members of IT, Premera refused to commit resources to implement the plan. Ex. 18 (Robinson) at 206:10-208:9.

g. Premera did not properly segment its network.

External auditors repeatedly noted deficiencies in Premera's network segmentation that could leave it exposed to greater risks of data theft. Network segmentation can "help contain incidents and support the security objectives of the organization through its design." Ex. 57 (Coalfire 30(b)(6)) at 89:3-13. Network segmentation allows a company "to isolate some of the different systems and data from each other." Ex. 58 (Murphy) at 152:15-22. Segmenting makes it

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

harder for a hacker to gain access to the entirety of a company's information if they are somehow able to breach part of the protected environment. Ex. 57 (Coalfire 30(b)(6)) at 91:25-92:4.

In a 2012 Premera audit, Accuvant found "gaps relating to network segmentation" relevant to Premera's security posture. Ex. 34 at PBC00000630. Premera had "limited access control mechanism implemented between the various network segments on the internal corporate network. There [was] also limited segmentation between different security tiers within this network, *potentially allowing attackers to move freely from inconsequential systems to highly sensitive areas*." *Id*. at PBC00000667 (emphasis added). By 2013, Accuvant's assessment was even more critical, increasing the risk level associated with segmentation issues from medium to high. Ex. 35 at PBC00000710, 771. Again, Accuvant warned that "once a system is compromised, adjacent systems can be targeted through traditionally less secure interior services to gain deeper access in the network if controls are not in place to isolate high-risk systems. A lack of strong segment and service access controls results in a larger attack surface and may allow an attacker to gain access to sensitive data assets." *Id*. at PBC00000771-72; *see also* Ex. 57 (Coalfire 30(b)(6)) at 91:25-92:4. In other words, once the hackers were in Premera's servers, they had free access to all of its confidential Sensitive Information.

Although the IT department was aware that network segmentation was critical to data security and had even created a network segmentation plan in 2013, Premera corporate would not give them the necessary resources, perhaps because it would have required a complete rebuild of the FACETS database. Ex. 18 (Robinson) at 206:10-208:22; Ex. 56.

h. Premera knowingly failed to patch and update its antivirus software and ran servers that lacked antivirus or antimalware.

Regular software patching is essential to IT security, and necessary to close exploitable security weaknesses in software applications. Ex. 28 (Vergeront) at 213:21-214:17; 242:21-

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

243:18. "Both targeted threat actors and criminals who deploy mass malware typically gain initial entry into an organization . . . [using] malware [that] exploits vulnerabilities in common third-party applications . . . ." Ex. 59 at PBC00258206; *see* Strebe Decl., Ex. B(r). Up through the time of the breach, Premera's internal and external auditors regularly noted critical deficiencies in both the timeliness and comprehensiveness of Premera's software patching. For example, external audits in 2011 "found weaknesses regarding patch management" and recommended Premera deploy a "more vigorous patch management policy." Ex. 30 at PBC00000160. External auditors continued to warn Premera of its inadequate patching in 2012 and 2013. Ex. 34 at PBC00000629-30; Ex. 35 at PBC00000711-12.

Yet Premera failed to take action to remediate its patching deficiencies. In December 2013, IA documented that Premera had not tracked or remediated the patching concerns identified in 2012, and that many of these issues retained their "high" criticality rating. Ex. 40 at PBC00164455. Premera's policies around patching were "poorly defined" and the "existing network patching process [was] not ensuring that security patches for network devices [were] being reviewed and applied in a timely manner." Ex. 60 at PBC00194473; Ex. 18 (Robinson) at 34:17-35:11 (application patching nonexistent). Failure to timely patch these vulnerabilities left exploitable entryways for hackers. Ex. 28 (Vergeront) at 242:21-245:6; Ex. 18 (Robinson) at 90:18-91:10 (failing to patch applications on endpoint leaves easily exploitable access point for hackers to access PHI).

In addition, Premera's antimalware and antivirus protection contained exploitable gaps. *See* Strebe Decl., Ex. B(c). Several of Premera's servers lacked antimalware and antivirus protection. In 2013, IA reported that 16 servers with internet access did not have antimalware installed. Ex. 61 at PBC_TAR00317128; *see also* Ex. 62. Similarly, in 2013, several Premera

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

employees discussed concerns about the fact that only half of Premera's servers had required antivirus software. Ex. 63. The gaps in Premera's patching, antivirus, and antimalware protection left critical holes in Premera's systems, inviting exploitation by malicious hackers. Indeed, missing patches were examined as a root cause of a malware infection at Premera in 2014. Ex. 28 (Vergeront) at 243:2-18. Yet management explicitly approved not updating servers with current antimalware. Ex. 18 (Robinson) at 104:20-106:10; 107:5-110:16.

i. Premera had poor phishing and security awareness.

Employee security awareness, including of phishing attempts, is a critical last line of defense against security breaches. *See* Strebe Decl., Ex. B(t). Although Premera did have a security awareness program that involved annual training, these efforts were largely ineffective. Numerous employees failed to complete "mandatory" training without consequences (including the individual who fell for the actual phishing scam that led to the May 2014 breach). Ex. 64. Moreover, employees continued to fail controlled phishing attempts. For example, in 2012, external auditors found that a significant number of targeted employees clicked on phishing links or provided credentials to unauthorized websites: 45% followed the provided link, 23% filled out a provided form, and 18% provided login credentials. Ex. 34 at PBC00000671-673. In 2013, the same external auditors had a 55% success rate in getting Premera employees to provide login credentials to a fake website—a substantial increase from the previous year. Ex. 35 at PBC00000768-770. In a similar investigation performed by another third party in 2014, of the 50 employees sent simulated phishing emails, 66% of employees clicked on the link and 32% provided login credentials. Ex. 36 at PBC00096313. Premera employees' high susceptibility to phishing attempts was "a statement of general company awareness and training." Ex. 36 at PBC00096299.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

j. Premera had inadequate password requirements.

Premera's lax password policies exacerbated its other security weaknesses, and left Premera at further risk for password harvesting, which the hackers exploited during the 2014 breach. Ex. 59. Auditors warned Premera for years that its password policies were weak and in need of improvement. In 2012, Accuvant Labs, found that "weak passwords and outdated software allowed the compromise of several hosts." Ex. 34 at PBC00000628. While Accuvant made a recommendation that Premera implement more complex and secure password requirements, Premera did nothing, and the same problems with "weak passwords" remained when Accuvant examined Premera one year later. Ex. 34; Ex. 35 at PBC00000733-734. In addition, IA found that Premera had too many service accounts that either had no passwords, or passwords that had not been changed in a long time, presenting a significant security risk. Ex. 18 (Robinson) at 32:17-33:9.

iii. Premera's dysfunctional IT department fostered a culture of denial and avoidance to hide its inadequacies.

Despite the numerous and repeated critical deficiency findings in Premera's data security systems that exposed it to increased risk of a data breach and placed it in violation of HIPAA, Premera employees routinely failed to report issues to superiors, actively sought to derail IA's attempts to identify deficiencies, and did not act with any urgency to remediate deficiencies prior to the discovery of the May 2014 data breach.

Employees failed to report known issues or concerns, either because they feared reprisal, wanted to use the knowledge for their own personal advancement, or sought to minimize the risks of the glaring security flaws. Ex. 24; Ex. 22; Ex. 18 (Robinson) at 151:8-152:17; Ex. 1 (Kemp) at 67:18-71:13, 78:12-79:5, 84:21-85:12, 91:2-95:22, 101:24-103:23, 106:3-113:6, 122:5-123:9. This behavior extended to IA investigations. IT security employees were hostile

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

toward internal auditors and were reluctant to provide the information necessary to assess Premera's security deficiencies. Ex. 42 (Klouzal) at 41:18-42:14, 43:1-4, 43:20-44:18; Ex. 66; Ex. 18 (Robinson) at 43:8-47:12; Ex. 67. Even external auditors noted that "the working relationship between IT and internal audit is not beneficial to the company." Ex. 68 at PBC00008444. Prior to discovery of the data breach, Premera employees reported to Human Resources that Eric Robinson had lied to IA during its investigation. Although Robinson has denied this accusation, the internal auditors received inconsistent statements from Robinson and his subordinates regarding Robinson's knowledge about the lack of IDS monitoring. Ex. 28 (Vergeront) at 197:20-198:25, 224:21-225:13. In fact, Robinson had a reputation for "saying different things to different people." Ex. 42 (Klouzal) at 118:9-119:5. And Robinson did admit to a lack of candor by misleading auditors with a "bait and switch" response during the 2014 audit investigation, and "erroneously minimiz[ing] the risk associated with" IDS-monitoring deficiencies. Ex. 18 (Robinson) at 165:6-167:25, 231:2-7; Ex. 23 at PBC_TAR00238917.

Premera's post-audit conduct was no better. When Premera received audit reports, the results were not disseminated amongst all IT security personnel, thereby preventing department members from having a complete picture of the state of Premera's data security. Ex. 13 (Christian) at 87:23-88:21, 92:19-93:20, 110:23-111:13; *see* Exs. 33-34. More troubling, however, is that Premera employees would promise to remediate issues, but fail to follow through. Ex. 42 (Klouzal) at 63:14-65:14, 115:18-117:17; Exs. 61, 69. Audits were repeatedly left open for a long time. Ex. 70 (noting final clearance of five network security issues, some of which had been open for 700 days). Likewise, IT would fail to do required tasks and then attempt to cover its tracks; for example, in 2013, IT was required to conduct monthly periodic reviews, but IA found they were "in fact performed just the month before the review (to show

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

that they knew they were supposed to be doing it)." Ex. 71 at PBC_TAR00297887; Ex. 42 (Klouzal) at 122:12-123:2.

C. Foreseeably, Premera's Inadequate Data Security Led to a Breach of its Systems and Theft of Sensitive Information

i. In May 2014, hackers exploited Premera's security flaws to gain access to Premera's entire network, including the database where Premera stores Sensitive Information; the hackers had undetected access to Premera's systems for eight months.

On May 5, 2014, hackers sent a "phishing" email to a Premera employee, falsely purporting to be from a Premera IT employee using a visible "@premrera.com" email address with an extra "r." Ex. 72; Ex. 73 (FireEye 30(b)(6)) at 95:9-96:3. The email provided the employee with a link to download a "Citrix Secure Input IE ActiveX Control" and instructed the employee to log-in to the "Citrix Virtual Workplace System to activate your account." Ex. 72; *see* Strebe Decl., Ex. B(f). In response to this email, the employee clicked on the link and downloaded software that was, in reality, malware that allowed hackers to access Premera's servers. Ex. 73 (FireEye 30(b)(6)) at 96:16-24. Poor segmentation of Premera's network allowed the hackers to quickly access all areas of Premera's databases, including the FACETS and other databases where Premera stored its claims information and other Sensitive Information. Ex. 74 (Seymour 30(b)(6), Sept. 21, 2017) ("Seymour Depo 2") at 42:8-16; Ex. 75 (Gowan) at 91:3-19. Because Premera did not encrypt its PHI on its internal network, this data was readily accessible to the hackers. Ex. 18 (Robinson) at 93:5-23. The hackers were able to view, access, and exfiltrate this Sensitive Information.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

ii. Premera's security team did not even discover the breach—a third party hired to investigate Premera's network after an outbreak of another malware infection discovered it.

In the fall of 2014, Premera experienced an outbreak of Zeus malware infections. Ex. 76 (Seymour 30(b)(6), Jan. 12, 2017) ("Seymour Depo 1") at 78:20-81:8; *see* Strebe Decl., Ex. B(ee). Premera engaged Mandiant to do a compromise analysis, given concerns about how extensive the Zeus infection had become. Ex. 76 (Seymour Depo 1) at 78:20-81:8; *see* Strebe Decl., Ex. B(l). Several months after Mandiant began its Zeus-related engagement, it found the hackers on Premera's systems. Ex. 74 (Seymour Depo 2) at 50:21-51:12. Thus, it was only by hiring an outside consultant to address a persistent (and apparently unrelated) malware issue that Premera discovered the significant data breach at issue here; none of Premera's IT security controls uncovered that hackers had been trawling through Premera's systems for months with unlimited access to the treasure trove of Sensitive Information that Premera stored in various databases.

iii. The hackers used RAR files to compress and exfiltrate massive amounts of Sensitive Information located on Premera's system.

Premera has publicly claimed to government regulators, and throughout this litigation, that it has "no evidence" of data exfiltration and thus no harm could have occurred as a result of the breach. Internally, Premera knows this narrative is false: all available evidence suggests that in spite of Premera's representations to the contrary, the hackers were able to view, access, and exfiltrate Sensitive Information. Strebe Decl. at ¶¶ 249-260, 274-280, 283-296.

In order to determine the extent of the breach and whether any data was stolen from Premera's servers, Premera engaged Mandiant to undertake a comprehensive assessment. During its investigation, Mandiant eventually uncovered the existence of "at least" seven deleted RAR files on Premera's servers (that had been created when hackers were accessing Premera's

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

system) totaling over 350 MB of compressed data (or up to 8.7 GB of uncompressed data). Ex. 77 at PBC00023966; Strebe Decl., Ex. B(y). This is equivalent to PII records for 5.5 million people. Strebe Decl. at ¶¶ 257-258. Even though the existence of such files is highly indicative of exfiltration, Premera never disclosed this crucial piece of information to the public, instead actively misleading them to believe that no such evidence exists. Premera's omission significantly increased the risk of future harm as breach victims have likely lowered their guards and relied on Premera's inaccurate public statements that would lead victims to conclude that no data had been exfiltrated.

The circumstances surrounding the existence of these unexplained deleted RAR files presents a strong likelihood that hackers extracted Sensitive Information from Premera's environment. Early in its investigation, Mandiant even told Premera that "the evidence suggests that the [deleted RAR] files were ***more than likely created by the attacker***." Ex. 78 at PBC00261226 (emphasis added). Moreover, in an evidence tag produced when Premera turned over forensic images of the servers that held the deleted RAR files to Mandiant, the "reason" identified in the chain of custody box on the form was: "Citrix server that was identified with ***staged .RAR files***." Ex. 79 (emphasis added). But Premera had an opportunity to edit Mandiant's report before it was finalized. *See, e.g.*, Ex. 73 (FireEye 30(b)(6)) at 263:6-13 (noting that "it's standard for us to deliver a draft report for comments and revisions to the client"). And it appears that at Premera's lawyers' request, Mandiant's conclusions that the hackers had created the RAR files were watered down and ultimately removed from the final Mandiant report that Premera now insists shows that there is no proof of exfiltration. *See id* at 263:6-13.

Despite Premera's duplicitous legal position, the existence of the deleted RAR files on Premera's servers is significant evidence that the hackers viewed and exfiltrated Sensitive

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Information from Premera's systems for multiple reasons: (1) hackers routinely use RAR files to compress and steal Sensitive Information; (2) the hacking group at issue here specifically targets PII data and has used RAR files for exfiltration in the past; (3) the manner in which the RAR files were created and then deleted to avoid detection are suggestive of exfiltration activity; and (4) Premera has no evidence that the RAR files were created by anyone other than the hackers. In addition, evidence from Premera employees and customers indicates that exposed Sensitive Information from Premera has already been widely misused.

a. Hackers commonly use RAR files to exfiltrate data.

It is commonly known within the cybersecurity community that when hackers need to remove harvested data from a system, they often compress it for efficient exfiltration and to avoid detection. Importantly, they frequently use the RAR format for such purpose. CrowdStrike, a cybersecurity consulting firm hired by several states investigating the Premera breach, confirmed the common use of RAR in data exfiltration and that discovery of such files warranted concern:[7]

> When an intruder wishes to exfiltrate data, the most common practice is to copy the data to a central location, compress the data to a single file, and copy that compressed file out of the network. ***The archive format most intruders use for this is RAR - a flexible, highly portable, highly compressed archive format that is not directly accessible on default configurations of most computers, offering some moderate protection from discovery . . .*** Hence, the presence of RAR files or evidence of related activity, coupled with their strong association with data exfiltration, typically warrants some concern.

[7] Premera unsuccessfully tried to weaken CrowdStrike's findings. *See* Ex. 81 at PBC00058014 (In comments to the draft CrowdStrike report, Premera objected to the language CrowdStrike used noting: "We do not believe that this is an accurate description of the Mandiant report. Mandiant was unable to determine whether the files were created by the intruder or Premera employees. Mandiant reached this conclusion because Premera employees used RAR files. This statement ignores this fact. Nonetheless, if this is CrowdStrike's opinion, then it needs to be made that it is Crownstrike's opinion.") [sic].

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Ex. 80 at PBC00168951(emphasis added); *see* Strebe Decl., Ex. B(i). Notably, Premera agreed with CrowdStrike's final conclusion that the presence of RAR files warrants concern. *See* Ex. 74 (Seymour Depo 2) at 87:13-20. Mandiant similarly acknowledged at deposition that attackers typically archive files to remove them from a system, in the exact same way as occurred here. Ex. 73 (FireEye 30(b)(6)) at 159:19-161:12 ("We typically look for large instances of [RAR or archive files] during investigations as *that's usually how attackers prefer to remove data from an environment* . . . .") (emphasis added).

b. The Chinese hacking group that breached Premera targets PII and uses RAR.

Chinese hackers are known to target PII and use RAR compression and extraction methods. The evidence here indicates that the actors responsible for the Premera breach were a Chinese Advanced Persistent Threat ("APT") group, which Mandiant has referred to as "Group A" (other researchers have dubbed them as "Deep Panda"). Ex. 73 (FireEye 30(b)(6)) at 256:16-267:10; Ex. 21 (Twitchell) at 175:2-17, 270:6-10; Ex. 82 (Seymour 30(b)(6), June 13, 2018) ("Seymour Depo 3") at 79:3-6; Ex. 83; Strebe Decl. at ¶¶ 263-273, *see* Ex. B(b). Mandiant and other security consultants agree that the APT group responsible for the Premera breach specifically targets companies hosting large amounts of Sensitive Information so that it can steal such data, uses RAR files for exfiltration, and was also likely responsible for the Anthem *and* OPM breaches, where similar data was stolen.

Prior to Premera's softening of Mandiant's conclusions, Mandiant even told Premera that the exact same Chinese group it found to have breached Premera's systems had already *exfiltrated* significant amounts of PII data from another one of Mandiant's unnamed clients. Ex. 84 ("Based on information I received from Mandiant's internal Intelligence team and other engagement leads, this threat actor [that caused Premera's breach] is at one or more of our

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

clients. ***At one of our clients, this attacker stole a large amount of PII data***. The attacker also gained access to the VPN and Citrix environment.") (emphasis added). This conclusion is what ultimately spurred Mandiant to begin a search for large files on Premera's servers and what led to the discovery of the deleted RAR files. *Id.* ("Based on this information, we have begun searching the servers for the presence of large file archives.").

Mandiant prepared a memorandum for Premera to provide to Congressional investigators identifying "Group A" as the likely hacker behind the attack and confirming that these types of "state-sponsored groups target and steal personally identifiable information (PII)" for espionage and financial gains, which can only be realized if the data is exfiltrated. Ex. 83 at FIREEYE007769 ("Cybercriminals can use detailed PII records, like those housed by healthcare companies, in several ways. The records are often worth more money in underground markets than stolen credit card numbers because the PII data can be used to mount more sophisticated financial crimes.").

Mandiant also linked "Group A" with the OPM data breach, in which government employee PII was stolen. Ex. 85 at FIREEYE0008226 ("We assess Group A to be behind many of the recent PII breaches, including most likely the OPM breach. . . . Group A appears to be specifically pursuing personal information. . . . [T]he targeting interest of Group A appears to have a noticeable emphasis on organizations that possess large amounts of personal data.").[8] In

[8] Other researchers have echoed Mandiant's conclusions that the same hackers were involved in the OPM, Premera, and Anthem breaches, particularly due to the similarities of the hacking methods involved. *See, e.g.*, David Perera, *Agency didn't encrypt feds' data hacked by Chinese - The hacker group, believed to be aligned with the Chinese government, has also been implicated in attacks on health insurers Anthem and Premera*, POLITICO (June 4, 2015), (https://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655); *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015) https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/; *see also Premera Blue Cross Breach Exposes Financial, Medical Records*, KREBSONSECURITY (March 17, 2015),

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

the OPM data breach, the hackers also used RAR files to exfiltrate data.[9] Importantly, the hack at OPM and attendant RAR-based data exfiltration has recently been linked to an *admitted* fraud scheme in Virginia.[10]

In short, the evidence shows that the Premera hackers were not pimply-faced teenagers out for a "joy ride" through Premera's systems; this was a sophisticated attack by a Chinese hacking group explicitly known for targeting and stealing sensitive PII and similar data from healthcare and other companies using RAR exfiltration methods. The fact that the same hackers targeted and exfiltrated data from similar hacks and that such data has now been found in the hands of criminals who used it to commit identity theft, is further evidence that they did the exact same thing at Premera.

---

https://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/.

[9] Brendan Koerner, Inside the Cyberattack That Shocked the US Government, Wired (Oct. 23, 2016) (emphases added) (available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/) ("The hunt turned up not just malware but also the first inklings of the breach's severity. A technician from the security software company Cylance, who was supporting the effort, spotted encrypted RAR files that the attackers had neglected to delete. He knew that RAR files are used to store compressed data and are often employed by hackers to shrink files for efficient exfiltration.").

[10] *See* Rachel Weiner and Derek Hawkins, *Hackers stole federal workers' information four years ago. Now we know what criminals did with it*, WASHINGTON POST (June 19, 2017) https://www.washingtonpost.com/local/public-safety/hackers-stole-feds-information-four-years-ago-now-we-know-what-criminals-did-with-it/2018/06/19/f42ff2b2-73d3-11e8-805c-4b67019fcfe4_story.html?utm_term=.bb1c021def68 ("Two people have admitted in Newport News federal court they used the stolen identities to take out fake loans through a federal credit union. The case appears to be the first involving OPM data to be publicly revealed by the Justice Department."); *U.S. v. Kariva Cross*, 4:17-cr-00118-AWA-DEM (E.D. VA, June 18, 2018) (Statement of Facts, Dkt. 93 p. 3) ("Investigators determined that many of the identity theft victims had been victims of the United States Office of Personnel Management data breach and resided in Colorado.").

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

c. The manner in which the RAR files were created and then deleted is indicative of exfiltration.

If the hackers did not create and delete the RAR files on Premera's servers, the only other potential explanation for their creation would be that a Premera employee or internal automated process created (and then deleted) them. There is no evidence that either occurred. To the contrary, there is ample evidence that the files could only have been created by the hackers.

As the Mandiant report explains, one of the compromised user accounts to which the hackers had access (referred to therein as "User Account 3") remotely logged in to the Premera Citrix server (MLTPBTSV6J or "6J") at 12:14 am PDT on Friday, June 6, 2014. Ex. 77 at PBC00023966. An hour later, at approximately 1:15 am, "at least" seven different RAR archives were created on this server consisting of approximately 350 MB of compressed data. *Id*. Mandiant could recover only the names of the files and could not determine their nature or content since they had been deleted. Nor could Mandiant determine whether additional RAR files had been created and deleted at this or other times. *Id*. And even though a hacker had remotely logged in (during the middle of the night, Pacific time) only an hour before the creation and deletion of these RAR files, because one other uncompromised account ("User Account 11") may have had access to the same directory where the RAR files were found, Mandiant stated that it could not determine whether a hacker or someone else created the deleted RAR files. *Id*. Mandiant also found residual evidence of the same RAR files, as well as a RAR archiving tool, on an entirely different server (MLTPBMX5A or "5A"). *Id*. at PBC00023967.

The obvious thing for Mandiant to do would have been to ask the employees assigned to User Accounts 3 and 11 whether either had created the RAR files. In interrogatory responses, Premera identified Marty Cookson as assigned to "User Account 3" and Harry Outlaw as assigned to "User Account 11." Ex. 86 at Interrogatory 7. While Mandiant never mentioned in its

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

report whether it questioned those employees, apparently Premera did ask Cookson and Outlaw and both denied having created or deleted the RAR files at issue. *Id.* at Interrogatory 11. Premera tried to attribute the creation of the RAR files to Netscaler server updates in its written interrogatory responses. *Id.* But Cookson admitted at his deposition that the only compression files related to Netscaler updates would be Windows compression (creating "ZIP" files), or "TAR" files, not RAR files. Ex. 87 (Cookson) at 31:9-33:8; 69:14-71:18. Cookson was also "not aware of any automatic or background processes under his control that could have resulted in the creation of a RAR file on the 5A Server." Ex. 86 at Interrogatory 11. Cookson further testified he did not create the RAR files at issue. Ex. 87 (Cookson) at 54:9-16. While Outlaw testified that he used the 6J server on June 6, 2014, according to Premera, he "did not use RAR files, did not create any RAR files, and is not aware of any process that would automatically create RAR files." Ex. 88 (Outlaw) at 16:7-25. Another Premera witness testified that despite Premera's interrogatory response to the contrary, Premera had long ago determined that the deleted RAR files were not related to Netscaler or Citrix updates. Ex. 75 (Gowan) at 161:13-162:3.

Nevertheless, Premera has gone to great lengths to create other explanations for the existence of the deleted RAR files, none of which withstand scrutiny. Premera has claimed an employee created these files *solely* based on the fact that the files had "VSD" in the name and Microsoft Visio (which creates "VSD" files) was used elsewhere in the Premera environment. Ex. 74 (Seymour Depo 2) at 65:23-66:4. Importantly, Premera found no other files on any of its systems with a "VSD" naming convention and could not identify a single Visio VSD file on the system (or even if the Visio software existed on its servers) to back up its claim. *Id*. at 61:13-16, 76:13-22. Cookson further testified he's never used that naming convention and does not know what it is. Ex. 87 (Cookson) at 43:8-15. Moreover, Mandiant acknowledged that it wouldn't have

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

mentioned the existence of the RAR files in its report if there was evidence the files had been created by a Premera employee. *See* Ex. 73 (FireEye 30(b)(6)) at 268:23-269:4 ("I think if a Premera employee created those RAR files that would be documented in this report, and we would not [be] talking about the RAR files, as they would be innocuous.").

When asked for "all bases for Premera's contention that it is more likely than not that data was not exfiltrated during the Data Breach," Premera's entire answer was:

> Mandiant's assessment regarding exfiltration in the Mandiant Report was that there was no evidence of exfiltration of data. The description of attacker activity suggests only investigation and reconnaissance activity, and no actual removal of data from the network. Premera has found no additional evidence of the exfiltration of data in its own investigation. The lack of a significant number of similar reports of identity theft from individuals whose information was potentially compromised also supports the inference that no data was exfiltrated, as does the lack of any outside evidence that data that could have been copied or removed from Premera's computer systems has been found to be in the hands of unauthorized persons.

Ex. 86 at Interrogatory 12. But, as detailed above, Mandiant's independent assessment was *not* that there was no evidence of exfiltration. In fact, Mandiant initially concluded that hackers had more than likely created the RAR files and their presence signified exfiltration. CrowdStrike made comparable findings to Mandiant's pre-edited conclusions of "attacker-staged RAR files," that the presence of these files "signified an increased likelihood that data was exfiltrated." Ex. 80 at PBC00168951.

Premera claims to have found no additional evidence of exfiltration in its own investigation, but its own investigation was woefully inadequate. Premera's 30(b)(6) representative could not answer crucial questions as to what Premera did regarding its "investigation," including whether it had compressed data through RAR to see what could have been in the files, or whether it looked to see if RAR compression was used in other breaches. Ex. 74 (Seymour Depo 2) at 29:1-30:11, 31:2-21, 49:23-50:1, 69:19-22. If Premera had done any of

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

these things, such information would have been produced or mentioned in other discovery answers.

iv. Premera's poor record keeping and destruction of evidence undermined attempts to investigate the breach and determine the extent of access and exfiltration.

Premera's own conduct has been the main impediment to determining conclusively what data was exfiltrated and the extent of such exfiltration. CrowdStrike confirmed that it was the result of Premera's own failures at identifying that a breach had occurred and the length of time that intruders were in the system that made it more difficult to conclude definitively whether data was exfiltrated. Ex. 80 at PBC00168961 ("The Premera breach was sufficiently long and the intruder had sufficient access to the environment that it would have been extraordinarily difficult to precisely enumerate all data the intruder accessed."); *see also* Strebe Decl. at ¶ 295 ("The lack of evidence of extraction occurred both because the hackers used tools designed to avoid detection, because Premera failed to maintain the logs necessary to show exfiltration, and because Premera was not competent to detect them.").

Various Premera security systems had the capability to record hacker activity, but at the time of the breach, Premera was not keeping logs from *any* of the following systems:

1) Intrusion detection system logs, which record hacker attempts to access Premera networks through improper means (Strebe Decl. at ¶¶ 103-104, 125-126);
2) Firewall logs, which record whether Premera allowed outsiders access to its network (Ex. 75 (Gowan) at 112:1-20; Ex. 89; Strebe Decl. at ¶¶ 110, 125-126, 172);
3) Proxy logs, which record requests users (including unauthorized users) made on Premera's network (Ex. 75 (Gowan) at 138:25-139:23; Strebe Decl. at ¶¶ 174-178, *see* Ex. B(w));
4) Data loss prevention logs from the Bluecoat software, which record authorized and unauthorized flow of Sensitive Information out of Premera's network (Strebe Decl. at ¶¶ 178, 189) (only DLP logs Premera produced were from an irrelevant period);

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

5) FACETS access logs, which record who and when users on Premera's network access or remove Sensitive Information from its FACETS claims database. Strebe Decl. at ¶¶ 210, 219, 245);
6) Bandwidth logs, which record the flow and volume of data out of Premera's network (Strebe Decl. at ¶¶ 162-165, 291; *see* Ex. B(d)).

Notably, HIPAA specifically required Premera to create and store FACETS access logs. 45 CFR §164.308(a)(1)(ii)(D); 45 CFR § 164.312(b). Premera's IT policies reflect this requirement. *See, e.g.* Ex. 50 at PBC_TAR00300216 ("Core EPHI Systems and domain controllers must log records of particular access events."); Strebe Decl. at ¶¶ 122-124.

Each of the above logs is crucial to a properly functioning IT security system and to a thorough investigation of a breach. Strebe Decl. at ¶¶ 50-51, 54-55, 203-206, 222. Together, adequate logs would show exactly when and where the hackers accessed Premera's systems and what Sensitive Information they accessed and exfiltrated. *Id*. at ¶¶ 41, 43, 158, 205, 223. Without these logs, any analysis of exfiltration is necessarily incomplete. Strebe Decl. at ¶¶ 240-247. Premera can only claim it has "no evidence of exfiltration" because its own deficient IT security system was not programmed to track and preserve this evidence. Ex. 86 at Interrogatory 12.

Premera also destroyed key evidence that would have shown exfiltration. In 2016 Premera destroyed one of the 35 machines that the hackers used in the attack, and its data is no longer available for inspection. Ex. 77 at PBC00023992-993; Ex. 90 at Interrogatory 14. Without the machine itself, no other source can show what the hackers did with this computer and what files or evidence of exfiltration (such as additional RAR compression files) the hackers may have left behind. Strebe Decl. at ¶¶ 225, 229. Premera also destroyed DLP system logs that would record sensitive information leaving Premera's system from the time that the hackers had access to its network in 2014. Ex. 91 at RFP 268. No other available source of data can show what DLP logs would: hackers transferring customers' Sensitive Information out of Premera's network

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

through logs showing data transfer. Strebe Decl. at ¶¶ 41, 43, 158, 205, 223, 240-247. Premera also destroyed *key* firewall logs, key pieces of evidence that could have shown "spikes" indicating that large files has been removed from Premera's system. Ex. 73 (FireEye 30(b)(6)) at 221:6-223:12; Strebe Decl. at ¶¶ 158, 170-173.

D. Despite Receiving Numerous Calls from Consumers Who Suffered Identity Theft and Medical Fraud, Premera Continued to Tell Its Customers, Employees, and the Public that It Had No Evidence of Exfiltration

Premera knew about the data breach for weeks yet failed to notify consumers that their data was potentially compromised until March 17, 2015. Ex. 92. In this notice, Premera revealed that its computer network was the target of "a sophisticated attack to gain unauthorized access to [its] Information Technology (IT) systems." *Id*. Notably, in an attempt to downplay the harm, Premera failed to disclose key information in its initial notice—omitting the fact that the breach had gone undetected for eight months, that it believed the attackers were from an Advanced Persistent Threat (APT) group that may have been based in China, and that there was evidence of exfiltration. In fact, Premera's primary focus in issuing its notice was on protecting its public image; it even went so far as to provide what its own employee acknowledged was a misleading quote to the Seattle Times claiming the OPM audit found its data security systems were adequate and HIPAA-compliant. Ex. 42 (Klouzal) at 139:3-141:1; Ex. 93.

Early after the investigation and announcement of the breach, Premera received numerous reports of suspicious activity and fraud that appeared to be breach-related. Nevertheless, Premera ignored, downplayed, and failed to document those reports, basing its decision to do so on the purported conclusions from Mandiant that there was no proof of exfiltration—conclusions which were modified by Premera in Mandiant's initial report. A partial and incomplete review of the call logs from Premera's consumer call centers set up after the

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

breach showed more than 400 troubling incidents of medical fraud, false prescriptions, and other types of fraud being reported by consumers. *See* Declaration of Cecily Shiel ("Shiel Decl.") at ¶¶ 2-7, Ex. A. Instead of recognizing these reports as evidence of exfiltration, Premera ignored them.

Premera employees were some of the first to indicate they had experienced fraud. One employee wrote an email to her superiors about the use of her *Premera-specific* information being utilized in an identity fraud situation: "I don't want to post online for my colleagues to read, but I can confirm that I have had identity theft. *My premera work phone number was used by someone who opened several credit accounts using my SSN*. . . . I thought someone 'in charge' might want to know this since *it may be true that data did get out*." Ex. 94 at PBC00038504 (emphasis added). After speaking with Premera's Executive Vice President of IT and Operations, Kacey Kemp, Premera employees were told not to track this information: "Ok. I just chatted with Kacey about this . . . . We're basing our understanding of whether or not data was removed from our systems on the forensic work being done by mandiant [sic] and the investigation being carried out by the FBI. *This is our source of truth- so we don't need to be tracking this information*." *Id*. at PBC00038502. Premera's "source of truth" was its own watered-down conclusions that it forced into the Mandiant report. Though Premera deliberately decided not to track these incidents, some evidence of these call records slipped through and there may well have been additional reports of PHI theft linked to the breach that went undocumented.

Not surprisingly, almost immediately after disseminating the Notice, Premera also began to receive calls from consumers whose data had been compromised. One Premera employee noted: "We are getting reports of suspicious activity from members, post attack. How should we

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

report these incidents to ensure we are responding and investigating as well as keeping a log?" Premera's IT staff responded with a tautology: "Our statement that data was not removed from our systems is based on the forensic investigation by Mandiant and the FBI. We have no evidence of inappropriate use of data." Ex. 95.

To address this influx of calls, Premera hired call centers at Orion, Epiq, and Black Swan. Ex. 96 at PBC_TAR00024067. In a "FAQ Tool" provided to Orion, Premera instructed customer service agents to tell thousands of callers that Premera knew of no "reports of identity theft or other fraud related to this incident" or "evidence . . . that the data [had] been used inappropriately." Ex. 97 at PBC_TAR00169534, 523. However, Premera knew from call center summaries that customers reported fraudulent tax filings, unauthorized bank charges, and medical charges for unrecognized services and prescriptions. A review of the call logs from Premera's call centers set up after the breach showed hundreds of troubling incidents of fraud being reported by consumers after the breach. Importantly, many of these complaints dealt specifically with medical and prescription related fraud involving information that could only be obtained from medical records, like those found in Premera's breached files. For example, a sample of these call logs include:

- "Received fax for a prescription from a provider in Canada. . . . [She] states she's never been to Canada and has never worn glasses"
- "[H]e got notification a prescription had been filled by a recognised DR but at a pharmacy he did not use" [sic]
- "[S]aid that someone got perscriptions in her name" [sic]
- "Member thinks someone has received service under their name . . . ."
- "Customer also stated that she received 2 bills for services she may not have received."
- "Has some charges or info on claims he doesn't recognize."
- Her SSN is pulling up someone else at the Dr.'s office/ Adv that she can see the Dr and give her the SSN/Mbr ID."
- "Claims there are services on EOB [Explanation of Benefits] that aren't theirs (Serenity Sleep Solutions)."
- "[R]eceived an eob and he said this is not him - connected to CS"

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

- "[S]aying that someone has hacked into his sons info and making claims against him"
- "Member called and has had fraudlent activity with doctor visits" [sic]
- "Cust had suspected fraud on medical account"
- "CALLED BECAUSE SHE BELIEVES SHE WAS A VICTIM OF FRAUD SHE RECEIVED A CALL FROM TOPICAL LLC. […] AND SHE HAS NEVER HEARD OF THEM AND THEY SAID THEY HAVE HER INFO FROM HER PROVIDER."
- "Calling about fraudulent medical charges on account. Gave Fraud Hotline number."
- "Wanting to report fraudulent medical claims. Gave Fraud Hotline number."
- "cust is recieveing bills from hospitals he has not attended" [sic]
- "Received 30 EOB's - Hospice Care but does not receive that care"
- "Said he received an EOB with services that he did not receive."
- "being charged for meds she does not take"
- "called in sd that gt letter frm hospital said that dghter wnt to hospital but she clled verify with hospital someone used her dghter imfo sd waiting on respnce from the hosptital"
- "He stated he received false billing that nobody was able to identify in the timeframe between May 4th, 2014 to Janurary 29th, 2015" [sic]

Shiel Decl., Ex. A. Stories like these abound and are further indication that the hackers exfiltrated Sensitive Information and sold it to fraudsters on the black market.

In addition to the over 400 reports from consumers of identity theft and medical fraud through Premera's call centers, Plaintiffs in this action personally experienced identity theft and fraud. For example, in June 2015, just after announcement of the breach, the same type of PII that Premera stored on its system was used to fraudulently open numerous lines of credit in Sharif Ailey's name. Ex. 98 (Ailey) at 42:1-48:21 (Macy's), 54:20-56:25 (Lowe's), 62:5-15 (Sam's Club), 66:22-67:23 (Citi), 69:20-24 (Best Buy), 72:4-13 (jewelry financing); Ex. 99 at 10. In February 2015, Elizabeth Black received notice from a cellular telephone provider that multiple mobile phones were ordered using her name, address, phone number, Social Security number, and date of birth. Ex. 100 (Black) at 29:10-32:9, 36:10-37:7, 42:20-43:3; Ex. 101 at 10-11; Ex. 102. Barbara Lynch learned in January and February 2015 that numerous financial accounts had been opened in her name without her authorization. Ex. 103 (Lynch) at 27:11-25; 29:24-30:24, 45:5-46:7, 69:6-71:21, 98:2-25, 114:7-15:25, 118:12-20:12. Gabriel Webster

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

suffered unauthorized charges on one of his credit cards in November 2014. Then, in February 2015, his family's federal income tax return was rejected because someone had already used their names, address, Social Security numbers, and dates of birth to file a fraudulent return. Ex. 104 (Webster) at 19:17-21:13, 27:20-31:11. Catherine Bushman suffered tax fraud following the data breach, in 2015 and again in 2016, and several credit cards were opened fraudulently in her name. Ex. 105 (Bushman) at 20:1-21:22, 33:12-34:16, 40:11-41:17, 46:18-47:9, 60:13-23. These types of stories are prevalent and are further indication that Premera's Sensitive Information has found its way in to the hands of fraudsters. *See also* Ex. 106 (Allred) at 22:22-25:15; 30:18-22, 32:19-33:4) (minor son's social security number was used to file tax return; had not been provided to another entity for any purpose other than insurance coverage; and had not been notified of being part of another data breach); Ex. 107 (Christopherson) at 43:1-55:22 (received phone phishing scam with checking account number); Ex. 108 (Hansen-Bosse) at 49:4-50:23, 58:4-61:25, 67:16-69:15 (automatic payments cancelled, account frozen, money diverted from account, credit score decreased, attempted car loan).

E. Premera Has Still Not Fully Remediated its Security Vulnerabilities, Putting Consumer Data at Further Risk of Exposure

Despite the money it has spent and improvements it has made to remediate the breach, Premera has still not fully corrected the deficiencies in its data security that led to the breach, and consumers' sensitive data is still at risk of exposure. For example, as of June 26, 2018, its new identity management software is still not in place. Ex. 58 (Murphy) at 63:4-64:17. Mr. Murphy doesn't know whether Premera's existing identity management software meets Mandiant's recommendation to strengthen passwords. *Id.* at 65:4-67:13; Ex. 109 at PBC00168847. Certain servers still do not comply with Mandiant's recommendation to secure and restrict the use of local administrator accounts on Windows systems, and Premera has not yet limited the number

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

of computers that high-privileged user accounts could access. Ex. 58 (Murphy) at 109:8-112:6, 112:13-114:7.

Most critically, Premera is not securely archiving offsite the personal data of current and former customers, nor is Mr. Murphy aware of plans to do so in the future. *Id.* at 126:1-127:25 Premera has recently instituted secure offsite archiving only for members of other non-Premera BCBS plans that haven't had a claim for more than three years. *Id.* Archiving is one of the easiest ways to reduce the number of people at risk of Sensitive Information loss in a breach and should be applied to all customer data. Strebe Decl. at ¶¶ 46, 108. Simply put, if the data isn't there, hackers can't steal it.

IV. LEGAL ARGUMENT

A. The Proposed Classes Satisfy the Elements of Rule 23(a)

The requirements of Federal Rule of Civil Procedure 23 are well known: numerosity, commonality, typicality, and adequacy, and satisfaction of the requirements for one of the class types defined in Rule 23(b). *Ellis*, 657 F.3d at 979-80. To certify a Rule 23(b)(2) class, the plaintiff must show that "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). Certification under Rule 23(b)(3) requires that "questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." *Sali v. Corona Reg'l Med. Ctr.*, 889 F.3d 623, 629 (9th Cir. 2018) (internal quotation omitted). Rule 23(c)(4) provides a court with discretion to certify a class to resolve particular issues, such that "[e]ven if the common questions do not predominate over the individual questions," a court may "isolate the common

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

issues . . . and proceed with class treatment of these particular issues." *Valentino v. Carter-Wallace, Inc*., 97 F.3d 1227, 1234 (9th Cir. 1996). Plaintiffs have met all of these standards here.

i. The members of the proposed classes are so numerous that joinder is impracticable.

To satisfy the numerosity requirement, the proposed class must be "so numerous that joinder of all members is impracticable." Fed. R. Civ. P. 23(a)(1). A putative class of at least forty members usually is sufficient to satisfy the numerosity requirement. *Oregon Laborers-Employers Health & Welfare Trust Fund v. Philip Morris, Inc.*, 188 F.R.D. 365, 372 (D. Or. 1998). At the time that the breach was finally remediated on March 6, 2015, Premera's network held the Sensitive Information of approximately 8,056,277 million current and former Premera members, and an additional 1,889,284 current and former non-Premera Blue Cross Blue Shield members for whom Premera administered health benefit claims. Ex. 110. Because the various proposed classes all contain hundreds of thousands if not millions of class members, each of the proposed classes satisfies the numerosity requirement.

ii. Numerous questions of fact are common to the classes.

Plaintiffs' claims all involve common questions of law and fact regarding Premera's data security. Commonality requires common questions that "generate common answers apt to drive the resolution of the litigation." *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011) (quotation omitted). To satisfy commonality, "[e]ven a single [common] question will do." *Id.* at 359 (edits in original) (citation omitted); *see also Ellis*, 657 F.3d at 981. Thus, "[w]hen the party opposing the class has engaged in some course of conduct that affects a group of persons and gives rise to a cause of action, one or more of the elements of that cause of action will be common" and the requirements of Rule 23(a)(2) are satisfied. *Phelps v. 3PD, Inc.*, 261 F.R.D. 548, 555 (D. Or. 2009) (quoting *Oregon Laborers*, 188 F.R.D. at 373).

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Plaintiffs' claims arise out of a common core of facts, and a determination of those claims necessarily rests on common factual questions. For example, whether Premera's data security practices were sufficient is a common question of fact imbedded in each one of Plaintiffs' claims. Moreover, this question will be answered using common evidence. As discussed, Premera held Sensitive Information for Premera members and Blue Members in centralized databases. Ex. 74 (Seymour Depo 2) at 42:8-16. Its security practices did not vary internally or among its members. Proof regarding Premera's (deficient) security practices will be common across the classes and this alone is sufficient to establish commonality. *See, e.g.*, *Grays Harbor Adventist Christian Sch. v. Carrier Corp*., 242 F.R.D. 568, 572 (W.D. Wash. 2007) (finding numerous common questions related to Washington CPA claim); *Smith v. Triad of Alabama, LLC*, 2017 WL 1044692, at *8 (M.D. Ala. Mar. 17, 2017), *on reconsideration in part*, 2017 WL 3816722 (M.D. Ala. Aug. 31, 2017) (holding, in data breach case, that "[t]he effect and terms of the purported contract are common points sufficient to carry the first claim past Rule 23(a)(2)").

In addition, other common questions include: (1) Whether Premera was aware or had reason to be aware that its systems were vulnerable to attack, given multiple government warnings and the inadequacies and deficiencies in its own data security policies and procedures; (2) Whether Premera violated HIPAA in its policies and practices regarding data security; (3) Whether Premera was unfair or deceptive in its business practices by failing to disclose deficiencies in its data security; (4) Whether the breach compromised Sensitive Information ; and (5) Whether Plaintiffs and the members of the proposed classes are entitled to damages as a result of Premera's conduct. These common questions run throughout all classes' claims.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

iii. Plaintiffs' claims are typical of the class.

Rule 23(a)(3) requires that "the claims or defenses of the representative parties are typical of the claims or defenses of the class."[11] Fed. R. Civ. P. 23(a)(3). "Under the rule's permissive standards, representative claims are 'typical' if they are reasonably co-extensive with those of absent class members; *they need not be substantially identical*." *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1020 (9th Cir. 1998) (emphasis added); *accord Meyer v. Portfolio Recovery Assocs., LLC*, 707 F.3d 1036, 1041-42 (9th Cir. 2012). Thus, "a plaintiff's claim is typical if it arises out of the same event or practice or course of conduct that gives rise to the claims of other class members and his or her claims are based on the same legal theory." *Phelps*, 261 F.R.D. at 557 (quoting *Sorenson v. Concannon*, 893 F. Supp. 1469, 1479 (D. Or. 1994)).

Plaintiffs' claims are typical of the proposed classes because Plaintiffs possess the same interests and suffered harm from the same conduct as did the members of the proposed classes. Plaintiffs' claims, and the claims of the members of the proposed classes arise out of Premera's practice of failing to implement adequate data security practices and concealing from its customers Premera's inadequate practices. The harm suffered by Plaintiffs and the proposed classes resulted "from the same, injurious course of conduct," and the damages and injunctive relief sought will provide relief to all class members. *Armstrong v. Davis*, 275 F.3d 849, 868-69 (9th Cir. 2001); *see also O'Donovan v. CashCall, Inc.*, 278 F.R.D. 479, 491-92 (N.D. Cal. 2011) ("[T]o the extent that Plaintiffs' claims stem from the same underlying conduct by [defendant] . . . there is a sufficient nexus between Plaintiffs' claims and those of the putative

[11] The typicality requirement "tend[s] to merge" with the commonality requirement. *Gen. Tel. Co. of the Sw. v. Falcon*, 457 U.S. 147, 157 n.13 (1982); *see also Sorenson v. Concannon*, 893 F. Supp. 1469, 1479 (D. Or. 1994) (analyzing the typicality and commonality requirements together and stating that these requirements are "not high").

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

class members" to satisfy the typicality requirement); *Kay v. Wells Fargo & Co.*, 247 F.R.D. 572, 578 (N.D. Cal. 2007) (typicality requirement met where claims "arise[] out of the same business practices"). The typicality requirement is met here.

iv. Plaintiffs and their counsel will adequately represent the proposed classes.

Rule 23(a)(4) requires that "the representative parties will fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a)(4). This requirement has two subparts: (1) that the proposed representative plaintiffs have no conflicts of interest with the proposed class; and (2) that plaintiffs are represented by qualified and competent counsel. *Phelps*, 261 F.R.D. at 558. Both of these prerequisites are satisfied here.

a. The proposed representative plaintiffs have no conflicts of interest with the proposed class.

Here, the interests of the Plaintiffs are identical to the interests of each member of the proposed classes they seek to represent. All members of each proposed class seek to recover damages and/or injunctive relief for Premera's wrongful conduct. There is nothing to indicate that the interests of the named plaintiffs are in conflict with that of any members of the class. Declaration of Tina Wolfson (re Appointment of Class Counsel) ("Wolfson Decl.") at ¶ 21. That only some Class members suffered identity theft does not create an "intraclass conflict." *See In re Target Corp. Customer Data Sec. Breach Litig.*, 892 F.3d 968, 974-75 (8th Cir. 2018) ("*Target II*"). Thus, Plaintiffs have satisfied adequacy.

b. Class counsel are qualified and competent.

The adequacy of any class counsel depends on whether counsel (1) has investigated the class claims; (2) is experienced in handling class actions and complex litigation; (3) is knowledgeable regarding the applicable law; and (4) will commit adequate resources to representing the class. Fed. R. Civ. P. 23(g). Here, proposed Class Counsel, Liaison Counsel, and

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

the Executive Committee are experienced class action attorneys, have been appointed to leadership positions in numerous class actions, and have experience litigating consumer, privacy, and data breach cases. They have vigorously prosecuted this case, investing the necessary human and financial resources, and will continue to do so until they achieve a successful resolution. Declaration of Keith S. Dubanevich at ¶¶ 3-9 ("Dubanevich Decl."); Declaration of James J. Pizzirusso at ¶¶ 2-4; Declaration of Karen Hanson Riebel at ¶¶ 3-5; Declaration of Kim D. Stephens at ¶¶ 2-4; Wolfson Decl. at ¶¶ 11-18.

B. Each of Plaintiffs CPA, Negligence, Breach of Contract and CMIA Classes Satisfy the Predominance and Superiority Requirements of Rule 23(b)(3)

Plaintiffs seek certification of four proposed classes under FRCP 23(b)(3), which requires that (1) common questions of law or fact predominate; and (2) a class action is superior to other methods available for the fair and efficient adjudication of the controversy. Plaintiffs' CPA, negligence, breach of contract, and CMIA claims each satisfy these requirements.

"The Rule 23(b)(3) predominance inquiry tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation." *Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 623 (1997). "Rule 23(b)(3) focuses on the relationship between the common and individual issues." *Phelps*, 261 F.R.D. at 559 (quoting *Hanlon*, 150 F.3d at 1022). "Plaintiffs need not establish that there are no individual issues, only that the class issues predominate and that a class action is superior." *Id.* (citing *Local Joint Exec. Bd. of Culinary/Bartender Trust Fund v. Las Vegas Sands, Inc.*, 244 F.3d 1152, 1163 (9th Cir. 2001)). "When common questions present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication, there is clear justification for handling the dispute on a representative rather than on an individual basis." *Hanlon*, 150 F.3d at 1022 (internal quotations omitted); *see also Local Joint Exec. Bd.*, 244 F.3d at 1162.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Courts analyze choice of law as part of the predominance inquiry. *See Mazza v. Am. Honda Motor Co., Inc.*, 666 F.3d 581, 589-90 (9th Cir. 2012). "[I]f the forum state's choice-of-law rules require the application of only one state's laws to the entire class, then the representation of multiple states within the class does not pose a barrier to class certification." *Johnson v. Nextel Commc'ns Inc.*, 780 F.3d 128, 141 (2d Cir. 2015).[12] In *Mazza*, the Ninth Circuit vacated an order granting class certification, holding that California's Unfair Competition Law did not apply nationwide, and therefore, because the law of multiple jurisdictions applied, the variances in state law overwhelmed common issues and precluded a finding of predominance for a single nationwide class. *Mazza*, 666 F.3d at 594, 596.

But here, under a proper choice of law analysis, the aggregated contacts with Washington overwhelmingly point to the application of Washington law for the CPA and Negligence Classes. And, unlike the claims at issue in *Mazza*, the Washington CPA does apply extraterritorially. *Thornell v. Seattle Serv. Bureau, Inc.*, 363 P.3d 587, 592 (Wash. 2015). A court is not required to conduct a 50-state choice of law analysis in a vacuum. And even Premera has argued for the application of Washington law to this case. *See* Def.'s Opposition to Pls.' Mot. to Compel, ECF No. 113 at 5 (arguing for application of Washington privilege law based on Premera's contacts with Washington). Further, the Court can apply California law to the CMIA Class and there is no meaningful difference in contract law for the Breach of Contract Class.

[12] The three-judge panel disposition in *In re Hyundai & Kia Fuel Economy Litigation* was recently vacated by the Ninth Circuit en banc and is thus not discussed herein. __ F. 3d __, 2018 WL 3597310 (9th Cir. July 27, 2018).

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

i. Common issues of law and fact predominate for the Washington CPA and Negligence Classes.

For the proposed CPA Class, Plaintiffs assert that Premera's misrepresentations about the safety of their Sensitive Information violated the CPA, and that Plaintiffs and the members of the proposed class are entitled to recover damages. "To establish a CPA violation, the plaintiff must prove five elements: (1) an unfair or deceptive act or practice that (2) occurs in trade or commerce, (3) impacts the public interest, (4) and causes injury to the plaintiff in her business or property, and (5) the injury is causally linked to the unfair or deceptive act." *Michael v. Mosquera–Lacy*, 200 P.3d 695, 698-99 (Wash. 2009) (citing *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 719 P.2d 531, 533 (Wash. 1986)); RCW § 19.86.020. "An unfair or deceptive act or practice need not be *intended* to deceive—it need only have the *capacity* to deceive a substantial portion of the public." *Deegan v. Windermere Real Estate/Ctr.-Isle, Inc.*, 391 P.3d 582, 587 (Wash. Ct. App. 2017) (emphasis in original) (quoting *Indoor Billboard/Wash., Inc. v. Integra Telecom of Wash. Inc.*, 170 P.3d 10, 18 (Wash. 2007)). Under Washington law, to prevail on a claim for negligence, a plaintiff must show "(1) the existence of a duty, (2) breach of that duty, (3) resulting in injury, and (4) proximate cause." *Ranger Ins. Co. v. Pierce Cty.*, 192 P.3d 886, 889 (Wash. 2008). All issues pertinent to these claims can be resolved on a classwide basis under Washington law, and thus, predominate over any individualized questions.

The Washington Supreme Court explicitly held that the CPA has extraterritorial reach, allowing out-of-state plaintiffs to assert claims under the CPA "against all persons who engage in unfair and deceptive acts that directly or indirectly affect the people of Washington." *Thornell*, 363 P.3d at 592. Here, there is no question that Premera's unfair and deceptive acts directly affect the people of Washington. Premera is a Washington-based company, the data at issue was

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

stored in the state of Washington, and all of Premera's conduct (or lack thereof) occurred in Washington. *See* Ex. 76 (Seymour Depo 1) at 67:11-68:2; Ex. 74 (Seymour Depo 2) at 58:12-60:7; Ex. 58 (Murphy) at 107:11-17; *see also Trader Joes Co. v. Hallatt*, 835 F.3d 960, 977 (9th Cir. 2016) (recognizing extraterritorial application of CPA and distinguishing application when defendants are not Washington residents). Accordingly, not only can the numerous Washington residents affected by Premera's conduct assert claims against Premera under the CPA, but so too can the proposed class members who reside outside of Washington.

The application of Washington law to the CPA and Negligence Class members on a nationwide basis is not only constitutional,[13] but appropriate under governing choice of law principles. *See Johnson*, 780 F.3d at 141 (noting where one state's laws can be applied to claims under choice-of-law rules, the involvement of multiple states does not pose a barrier to certification); *In re Qualcomm Antitrust Litig.*, 292 F. Supp. 3d 948, 978 (N.D. Cal. 2017) (same). And because only a single state's law should apply, there is no risk that individualized inquiries under competing state laws will predominate over common questions.

a. Washington law should apply to nationwide CPA and Negligence Classes.

Choice of law principles support application of Washington law on a classwide basis for both the CPA and negligence claims in this case. "In multi-district litigation, the district court must apply the choice-of-law rules that govern in the forum from which each particular lawsuit

[13] The application of Washington law also meets all constitutional prerequisites. To the extent there are any material conflicts between Washington law and the laws of any other state, the facts establish a "significant contact or significant aggregation of contacts" with Washington; specifically, all of Premera's conduct occurred in Washington and Premera cannot claim that the application of Washington law would be arbitrary, unfair or unforeseeable. *See Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 818, 820-21 (1985); *Kelley v. Microsoft Corp.*, 251 F.R.D. 544, 550 (W.D. Wash. 2008); *In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482, 486-87 (D. Minn. 2015) ("*Target I*").

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

was transferred (i.e., in law of the state where the suit was filed)." *In re United Parcel Serv., "Air-In-Ground" Mktg. & Sales Practices Litig.*, 580 F. App'x 543, 544 (9th Cir. 2014), *as amended* (July 25, 2014); *In re Korean Air Lines Co., Ltd.*, 642 F.3d 685, 700 & n.12 (9th Cir. 2011); *see also In re Nucorp Energy Sec. Litig.*, 772 F.2d 1486, 1491-92 (9th Cir. 1985). Here, while the consolidated complaint includes Plaintiffs from cases originally filed in district courts in Washington, Oregon, and Alaska, the only Plaintiffs that seek to be Lead Plaintiffs in the CPA and Negligence Classes are individuals who filed in the Western District of Washington. The Court should therefore conduct a choice of law analysis under Washington's choice of law rules.[14] *In re Takata Airbag Prods. Liab. Litig.*, 193 F. Supp. 3d 1324, 1334 (S.D. Fla. 2016) (conducting choice of law analysis under law of forum of named plaintiffs).

The first step in the choice of law analysis under Washington law is to determine whether there is a conflict between its law and the proposed law of another state. *Seizer v. Sessions*, 940 P.2d 261, 264 (Wash. 1997) ("[T]here must be an actual conflict between the laws or interests of Washington and the laws or interests of another state before Washington courts will engage in a conflict of laws analysis."). Here, where potential class members reside in each of the fifty states and U.S. territories, the existence of a conflict between Washington law and any other state will suffice for purposes of determining whether a complete choice of law analysis is appropriate. *Kelley v. Microsoft Corp.*, 251 F.R.D. 544, 550-51 (W.D. Wash. 2008), *certification withdrawn*, No. C07-0475 MJP, 2009 WL 413509 (W.D. Wash. Feb. 18, 2009) (finding conflict between

[14] To the extent the Court is inclined to apply the choice of law analyses of every transferor-court implicated in this MDL, the result is identical because each of the transferor forum states utilize the same choice of law tests. *Compare Yoshida's Inc. v. Dunn Carney Allen Higgins & Tongue LLP*, 356 P.3d 121, 130 (Or. Ct. App. 2015); *with Savage Arms, Inc. v. W. Auto Supply Co.*, 18 P.3d 49, 53 (Alaska 2001); *and Aetna Cas. & Sur. Co. v. Huntington Nat. Bank*, 587 So. 2d 483, 486 (Fla. Dist. Ct. App. 1991), *aff'd*, 609 So. 2d 1315 (Fla. 1992).

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Washington CPA and Illinois consumer protection statute). Plaintiffs recognize that Washington's CPA and negligence law may conflict with the consumer protection and, under certain circumstances, the negligence laws of some other states.[15]

When there are material conflicts between consumer protection statutes, this court determines what law should apply to Plaintiffs' claims pursuant to Washington choice of law rules, namely the "most significant relationship" rule as set forth in Restatement (Second) of Conflict of Laws ("Restatement") § 145. *Pruczinski v. Ashby*, 374 P.3d 102, 108 n.7 (Wash. 2016). That section[16] provides that contacts to be examined include:

> (a) the place where the injury occurred,
> (b) the place where the conduct causing the injury occurred,
> (c) the domicil, residence, nationality, place of incorporation and place of business of the parties, and
> (d) the place where the relationship, if any, between the parties is centered.
>
> These contacts are to be evaluated according to their relative importance with respect to the particular issue.[17]

Washington law has the most significant relationship to both Washington and non-Washington plaintiffs alike. The only potentially relevant locations for claims brought by non-

[15] For example, the Washington CPA materially conflicts with equivalent consumer protection laws in Oregon. *See* Oregon Unfair Trade Practices Act ("OUTPA"), Or. Rev. Stat. § 646.605 *et seq.* First, the CPA allows consumers to bring claims against insurers, whereas the OUTPA does not. Or. Rev. Stat. § 646.605(6). Washington negligence law conflicts with the laws of at least one other state. Unlike some states, Washington does not adhere to the economic loss doctrine, which would bar recovery for purely economic losses for tort claims under some circumstances. *See Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1150 (W.D. Wash. 2017) (finding conflict between negligence law in Washington and Iowa based on application of economic loss doctrine).

[16] Restatement (Second) of Conflict of Laws § 6 provides factors underlying the analysis under sections 145 and 148, including: (2)(b) "the relevant policies of the forum," (2)(d) "the protection of justified expectations," and (2)(f) "the certainty, predictability and uniformity of result."

[17] In cases involving deception by omission, courts will also look to Restatement (Second) of Conflict of Laws § 148. This section includes additional factors including the place whether the tangible thing which is the subject of the transaction was situated at the time.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Washington residents will be (1) Washington, where Premera is located and the injury-causing conduct occurred, and (2) the state of residence where each plaintiff suffered injury as a result of Premera's conduct. Here, Premera's incorporation and place of business is Washington. *See* Restatement § 145(2)(c). Premera stored the Class members' data on servers in Washington, regardless of where the Class member resided. Moreover, Premera's data security conduct occurred in Washington, and to the extent they are relevant, all of Defendant's misleading actions emanated from Washington. *See id.* §§ 145(2)(b), 148. Moreover, Washington has a clear interest in ensuring that its statutory regime and common law are applied to Washington businesses to deter unlawful conduct. *See id.* § 6(2)(c).

Premera's location and conduct in Washington outweighs the fortuitous contacts with other jurisdictions arising from class members' residence. Indeed, the location of an injury in a deceptive trade practices case or negligence case is substantially less significant than the state where the fraudulent conduct occurred. "When the injury occurred in two or more states, or when the place of injury cannot be ascertained or is fortuitous . . . the place where the defendant's conduct occurred will usually be given particular weight in determining the state of the applicable law. *Id.* § 145 cmt. e. Here, the hackers stole class members' data from Premera's servers in Washington due to Premera's deficient data practices in Washington; the locations where that data was fraudulently used or where plaintiffs felt harm were mere happenstance. Indeed, once individuals have had persistent identifiers exposed in a breach, they will be at increased risk of harm indefinitely; the effects of the breach could follow the class members for years to come and follow them around the globe. Van Dyke Decl. at ¶¶ 27-28.

The *Kelley* case out of the Western District of Washington is particularly instructive. In *Kelley*, the plaintiffs sought certification of a nationwide class under the CPA for deceptive acts

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

regarding the marketing of the Windows Vista operating system. 251 F.R.D. at 548-49. After finding that the CPA conflicted with at least one other state's laws (in that case, Illinois), the court conducted a "most significant relationship" choice of law analysis pursuant to Washington law under both Restatement § 145 and § 148. *Id.* at 551-52. Going through the list of factors, the *Kelley* court noted that while the putative class received and/or relied on the misrepresentations and the place of their injuries was nationwide, the defendant's acts occurred in Washington, the domicile of a named plaintiff and the defendant was Washington, and the relationships between the parties was not centered anywhere because the parties had not contracted with each other. *Id.* Although there were contacts with all 50 states, the court found "that the most significant contacts in the context of Plaintiffs' claims are to Washington, where Defendant resides and created the allegedly unfair or deceptive marketing scheme. Moreover, because the place of injury is fortuitous the Court gives greater weight to Washington, the location of the source of the injury." *Id.* at 552. The court was further persuaded by the fact that "Washington has a unique and substantial relationship with Defendant, one of Washington's largest corporate citizens, and the acts complained of by Plaintiffs took place in Washington." *Id.* at 553.

In other nationwide data breach cases, courts have applied similar reasoning to apply the law of one state to a nationwide class where the place of injury was fortuitous. In *In re Target Corporation Customer Data Security Breach Litigation*, the court held that Minnesota law applied to all class members' negligence claims because Target was incorporated and headquartered in Minnesota; the relevant servers affected by the breach were located in Minnesota; security decisions were made in Minnesota; and Target employees' failure to heed specific warnings about security vulnerabilities occurred in Minnesota. No. 14-2522 (PAM/JJK), 2015 WL 5996864 (D. Minn. Aug. 20, 2015) (trial memorandum); *see also Veridian*, 295 F.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Supp. 3d at 1153-54 (finding Washington had most significant relationship where misconduct related to defendant's decisions concerning internal data security that led to a data breach were made "at its corporate headquarters in Bellevue, Washington," and its failure to employ adequate data security measures "emanated from [its] headquarters" even though plaintiff was located in Iowa).[18]

The analogy to the claims in this case is virtually identical: a fortuitous, nationwide injury caused by Premera's—one of Washington's largest insurance companies—unfair and deceptive trade practices and negligent conduct that took place in Washington. This conclusion is further supported by the fact that Premera did not direct its actions at any specific consumers, but instead injured all class members simultaneously through its Washington-based conduct. Indeed, because its tortious conduct was uniform, Premera could reasonably foresee and anticipate that it would be held to Washington's laws with respect to all injured parties. *See* Restatement § 6(2)(d); *In re Target Corp. Customer Data Sec. Breach Litig*., 309 F.R.D. 482, 486 (D. Minn.

[18] Significantly, other courts analyzing choice of law issues in the context of data breaches have found the location of the conduct to be determinative. *See SELCO Cmty. Credit Union v. Noodles & Co.*, 267 F. Supp. 3d 1288, 1292 n.1 (D. Colo. 2017), *appeal dismissed*, No. 17-1289, 2017 WL 7668565 (10th Cir. Nov. 20, 2017) (finding Colorado law applied where no conflicts between potentially applicable laws, but noting that in case involving data breach, more weight is afforded the location of the conduct than the fortuitous location of the injuries); *Willingham v. Glob. Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *14-15 (N.D. Ga. Feb. 5, 2013) (applying law where defendant was domiciled, not where injury occurred where "Defendant's principal place of business is in Georgia, the data breach occurred in Georgia, and to the extent, if any, Defendant breached a duty to consumers, it did so in Georgia"); *First Choice Fed. Credit Union v. The Wendy's Co.*, No. 16-506, 2018 WL 2729264, at *6-7 (W.D. Pa. May 9, 2018) (applying Ohio law to negligence claim, based "on the actions and inactions of Defendants in safeguarding payment card data which was compromised in the hacking incident"); *Nat'l Union Fire Ins. Co. of Pittsburgh v. Tyco Integrated Sec., LLC*, No. 13-CIV-80371, 2015 WL 3905018, at *13 (S.D. Fla. June 25, 2015) (applying Florida law despite fact that injury occurred in Connecticut where defendant was headquartered in Florida, maintained computer servers in Florida and "more likely than not, Tyco's failure to safeguard the information is an event that took place in Florida").

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

2015). Moreover, Premera obtained PII from non-Washington residents either because they were employees covered under a Premera-issued insurance plan or were members of other BCBS plans that received treatment in Washington State with Premera-network providers. Ex. 1 (Kemp) at 14:3-24:25. The relationship between Premera and each class member was therefore centered in Washington State, and Washington law should apply.[19]

b. Other common issues of law and fact predominate for the Negligence and CPA Classes.

Other issues regarding Defendant's uniform conduct with respect to the CPA and negligence claims will predominate over any individual concerns. Courts in the Ninth Circuit have held that the predominance factor is easily met in consumer class actions where, for example, there are common questions as to "whether the defendants' standardized conduct . . . amounts to actionable misrepresentations . . . ." *Schwarm v. Craighead*, 233 F.R.D. 655, 663-64 (E.D. Cal. 2006) (citing *Amchem*, 521 U.S. at 625 ("[P]redominance is a test readily met in certain cases alleging consumer . . . fraud . . . ."). Similarly, predominance has been found in negligence cases, as well. *See Target I*, 309 F.R.D. at 487 (predominance met for negligence class under Minnesota law in data breach class action).

[19] Even if the weight of the contacts with other jurisdictions were equally balanced, other choice of law considerations require the application of Washington law. When the contacts between two jurisdictions are evenly balanced, the court must determine whether "some other state has a greater interest in the determination of a particular issue than the state where the injury occurred." *Kelley*, 251 F.R.D. at 553. In addition to affording greater weight to the location of the tortious conduct where the location of the injury is fortuitous, the Restatement provides that where "the primary purpose of the tort rule involved is to deter or punish misconduct [and not merely to compensate the victim for her injuries] . . . the state where the conduct took place may . . . [have the] most significant relationship." *Id.* (quoting Restatement § 145, cmt. c). Here, the CPA and negligence claims are both intended to deter future tortious conduct—indeed, plaintiffs seek injunctive relief on this basis. Washington has a particular interest in deterring unfair practices and negligence of Washington companies under the CPA that is superior to the interests of other states. *See id.*; *Thornell*, 363 P.3d at 592.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

Liability issues related to Plaintiffs' CPA and negligence claims will predominate. Premera's failure to disclose material deficiencies in its data security in the context of its business and the representations that it made to the members of the proposed Classes were materially identical. *See, e.g.*, Exs. 5, 6.[20] Given Premera's numerous failures to provide adequate data security, Premera's promises that it "must take measures to protect the privacy of your personal information" under HIPAA, that it "protects[s] your personal information in a variety of ways," and that it "takes steps to secure . . . electronic systems from unauthorized access" are unfair and deceptive to the class. Defendant sold health insurance policies that were supposed to comply with HIPAA's data security requirements. And Premera uniformly failed to tell its members that its security practices did not meet these expected standards. Premera's failure to disclose the truth about the security of Plaintiffs' and the proposed class members' Sensitive Information harmed every member of the proposed classes in the same way, as all members of the proposed classes were subject to Premera's common and deficient procedures and practices regarding data security. Premera held the same types of Sensitive Information for all the members of the proposed classes and stored that information centrally and managed that information in the same way.

The common factual and legal issues relating to whether the CPA Class Members suffered an injury to "business or property" caused by Premera's deceptive trade practices and their resulting damages, can be adjudicated on a classwide basis and therefore predominate over any individualized inquiries. Under the CPA, "injury" is not synonymous with damages. *Sorrel v. Eagle Healthcare, Inc.*, 38 P.3d 1024, 1028-29 (Wash. Ct. App. 2002) (finding CPA injury

[20] *See also* Premera, Code of Conduct 12 (2016), *available at* https://www.premera.com/documents/030553.pdf.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

where company failed to refund plaintiff's money for two weeks). Indeed, to satisfy the injury to business or property element of a CPA claim, a plaintiff need not even prove a specific monetary amount of damages. *Nordstrom, Inc. v. Tampourlos*, 733 P.2d 208, 211 (Wash. 1987); *Panag v. Farmers Ins. Co. of Wash.*, 204 P.3d 885, 899 (Wash. 2009). And as noted, cases interpreting the Washington CPA have found that there is a presumption of reliance for cases based on omissions. *Deegan*, 391 P.3d at 589-90; *Schnall v. AT & T Wireless Servs., Inc.*, 259 P.3d 129, 137 (Wash. 2011); *Davidson v. Apple, Inc.*, No. 16-CV-04942-LHK, 2018 WL 2325426, at *16 (N.D. Cal. May 8, 2018) (noting that "federal and state cases interpreting the WCPA" have found "a rebuttable presumption of reliance" for omission cases which "renders causation unproblematic"). Under this framework, whether Plaintiffs and class members suffered a cognizable injury under the CPA will depend entirely on the resolution of common questions of law and fact.

As with the CPA Class, the uniform application of Washington negligence law to all Negligence Class members eliminates any potential for individualized questions of law to predominate. Likewise, the legal and factual questions relating to the duties Premera owed to class members and the breaches arising from its failure to safeguard Plaintiffs' confidential data are identical with respect to each class member. *See Ranger Ins.*, 192 P.3d at 889 (elements 1-2).[21] Thus, these issues also predominate.

[21] Plaintiffs anticipate that Premera will argue that individual plaintiffs' injuries were the result of other data breaches, creating individualized questions of proximate cause. But Washington law allows for defendants to be liable in circumstances where there are more than one, concurrent, or subsequent proximate causes of an injury. *See, e.g.*, *Travis v. Bohannon*, 115 P.3d 342, 347-48 (Wash. Ct. App. 2005); 6 Wash. Prac., Wash. Pattern Jury Instr. Civ. WPI 15.04 (6th ed.).

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

With respect to damages, class issues predominate as well. The calculation of damages arising from Premera's unfair and deceptive trade practices or negligence are easily calculable on a classwide basis, as explained below. *Vaquero v. Ashley Furniture Indus., Inc.*, 824 F.3d 1150, 1155 (9th Cir. 2016) ("the need for individualized findings as to the amount of damages does not defeat class certification."); *Leyva v. Medline Indus. Inc.*, 716 F.3d 510, 514 (9th Cir. 2013).

Benefit of the Bargain Damages. If Plaintiffs establish their claims for liability, a jury will necessarily conclude that Plaintiffs purchased one product (health care with adequate security) but received a much less valuable one (health care without it). Plaintiffs would thus be entitled to recover damages equal to the value of the security services Premera failed to provide. *See, e.g., In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 985-86 (N.D. Cal. 2016) (recognizing such damages in a data breach under California law); *Matheny v. Unumprovident Corp.*, 594 F. Supp. 2d 1212, 1226 (E.D. Wash. 2009) (awarding benefit of the bargain damages to plaintiff under CPA against insurer who misrepresented policy benefits and provisions). To support their claim for this type of damages, plaintiffs attach the declaration of Professor Peter E. Rossi, the Collins Distinguished Professor of Marketing, Economics, and Statistics at UCLA, who explains how to calculate these damages on a classwide basis. *See* Declaration of Peter E. Rossi at ¶¶ 13-14.

Loss of Value of Sensitive Information. Plaintiffs will prove to a jury that Premera allowed hackers to access class members' Sensitive Information. Accordingly, plaintiffs will be entitled to recover the economic value that they lost because Premera exposed that information. *See In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617, 2016 WL 3029783, at *14-15 (N.D. Cal. May 27, 2016) (recognizing value in PII and that plaintiffs could be injured by loss of value of PII following breach); *see also* Bazelon Decl. at ¶ 7 (explaining why a person suffers

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

economic loss when his or her PII or PHI is stolen).[22] To explain how to calculate such damages on a classwide basis, plaintiffs attach the declaration of Dr. Bazelon, a principal at the well-respected Brattle Group economic consultancy. *See* Bazelon Decl.

Credit Monitoring. Additionally, whether as a form of injunctive relief or damages, plaintiffs contend that they are entitled to credit monitoring and insurances services for a reasonable number of years, or a remedy equal to the cost of maintaining these services. As the cost of credit monitoring is static, it can be calculated on a classwide basis. Declaration of Tina Wolfson (Re Classwide ID Monitoring and Insurance Damages) ("Wolfson Damages Decl."), Ex. 1.

ii. Common issues of law and fact predominate for the Breach of Contract Class.

Common issues of law and fact predominate the breach of contract claims. Although the claims will involve individual contracts issued in three states (Washington, Oregon, and Alaska), the laws of those states and the contractual language at issue do not materially conflict such that individual issues predominate. Moreover, the common liability and damages issues relevant to the contract claims predominate over any individual issues.

The contract claims are all based on promises Premera made in the Notice of Privacy Practices it sent to its members. This Notice included identical promises to all class members that Premera is "committed to maintaining the confidentiality of your medical and financial information," "must take measures to protect" members' data, and "take steps to secure [its] buildings and electronic systems from unauthorized access." Exs. 5, 6. Whether this Notice was incorporated by reference into the members' contracts is a common issue of fact, as Premera had

[22] Premera recognizes that even de-personalized PII is a valuable economic asset. Ex. 111 at RFA 2.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

a uniform practice of mailing the notice along with the policy booklet contract. Ex. 7; *see also In re Premera Blue Cross Consumer Data Sec. Breach Litig.*, No. 3:15–md–2633–SI, 2017 WL 539578, at *10-11 (D. Or. February 9, 2017) (citing *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2016 WL 754731, at *4-6 (ND. Ill. Feb. 23, 2016)) (holding that concurrent receipt of the Privacy Notice with the policy booklet was sufficient to state a claim for breach of contract based on the Privacy Notice).

Additionally, common issues of law predominate, as the breach of contract law claim is based on blackletter common law that does not vary in any meaningful respect from state to state.[23] Premera only issued insurance policies to companies and individuals in the states of Washington, Alaska, and Oregon. Ex. 1 (Kemp) at 151:21-152:22, 17:5-22. Several of these policies contain choice of law clauses specifying the application of Washington or Alaska law to contract claims. *See, e.g.*, Ex. 112 at PBC00009460 (Washington); Ex. 113 at PBC00012664 (Alaska). But in all three states, the goal of contract interpretation is to ascertain the parties' intent, which may be gleaned from extrinsic evidence or context. *Compare Yeager v. Philadelphia Indem. Ins. Co.*, No. 3:14-CV-00023 JWS, 2015 WL 3648860, at *4 (D. Alaska June 10, 2015); *W. Wash. Corp. of Seventh-Day Adventists v. Ferrellgas, Inc.*, 7 P.3d 861, 865-66 (Wash. Ct. App. 2000); *Complete Distribution Servs., Inc. v. All States Transp., LLC*, No. 3:13-CV-00800-SI, 2015 WL 5764421, at *5-6 (D. Or. Sept. 30, 2015). In addition, all three states favor interpretation of an insurance contract from the insured's point of view. *Compare Yeager*, 2015 WL 3648860, at *4; *Pac. Ins. Co. v. Catholic Bishop of Spokane*, 450 F. Supp. 2d

[23] The law for breach of contract does not vary materially by state. *See, e.g., Am. Airlines, Inc. v. Wolens*, 513 U.S. 219, 233 (1995); *In re U.S. Foodservice Inc. Pricing Litig.*, 729 F.3d 108, 127 (2d Cir. 2013) ("A breach is a breach is a breach, whether you are on the sunny shores of California or enjoying a sweet autumn breeze in New Jersey." (citation omitted)).

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

1186, 1197 (E.D. Wash. 2006); *Veloz v. Foremost Ins. Co. Grand Rapids, Michigan*, 306 F. Supp. 3d 1271, 1275 (D. Or. 2018). All three states allow for a contract to incorporate other documents by reference. *Compare Arnett v. Bank of Am., N.A.*, 874 F. Supp. 2d 1021, 1030 (D. Or. 2012); *Satomi Owners Ass'n v. Satomi, LLC*, 225 P.3d 213, 225 (Wash. 2009); *Prichard v. Clay*, 780 P.2d 359, 361-62 (Alaska 1989). Accordingly, these claims can be adjudicated on a classwide basis.[24] Indeed, the claim for breach of a "form contract . . . present[s] the classic case for treatment as a class action." *In re Scotts EZ Seed Litig.*, 304 F.R.D. 397, 411 (S.D.N.Y. 2015); *see also In re U.S. Foodservice Inc. Pricing Litig.*, 729 F.3d at 124 (affirming class certification where, as here, each proposed class member was subject to the same material contractual terms).

The issue of whether Defendant breached identical contractual language through its uniform conduct that resulted in a failure to maintain the security of Plaintiffs' confidential information, requires common proof and predominates over any potential individualized inquiry. Moreover, Plaintiffs' damages can be calculated on a classwide basis under the lost benefit of the bargain theory as a measure of plaintiffs' expectation damages, or under the loss of value theory as a measure of Plaintiffs' consequential losses foreseeably incurred by reason of Premera's contractual breach. *See supra*.

iii. Common issues of law and fact predominate for the CMIA Class.

California's Confidentiality of Medical Information Act ("CMIA") prohibits entities such as Premera from negligently releasing an individual's confidential medical information and

[24] To the extent the court finds material differences in the application of these three states laws, individual statewide classes would be appropriate and manageable. Thus, in the alternative, Plaintiffs ask the Court to certify state-specific contract classes for policies issued in Washington, Oregon, and Alaska. The Privacy Notice language is uniform for all class members, as is Premera's standard mailing practices for the Notices. Exs. 5-7.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

obligates a covered entity to treat such medical information in a "manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code §§ 56.36, 56.101(a); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1201 (D. Or. 2016). To establish a violation of the CMIA, a plaintiff must show that the defendant negligently caused the release of "individually identifiable information . . . regarding a patient's medical history, mental or physical condition, or treatment," and that an unauthorized third party "viewed or otherwise accessed" the confidential information. Cal. Civ. Code § 56.05(j); *Regents of the Univ. of Cal. v. Superior Court*, 220 Cal. App. 4th 549, 554, 564-65, 163 Cal. Rptr. 3d 205, 208, 216 (2013). In the context of the CMIA, a "release" need not be an affirmative, communicative act, but can be accomplished by "negligently allowing information to end up in the possession of an unauthorized person." *Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1554-55, 174 Cal. Rptr. 3d 653, 659 (2014). This claim can be tried under California law for a class of California residents, and the common issues to be tried predominate over any individual legal issues.

a. California law should apply to the CMIA Class.

The CMIA protects California residents' right to privacy in their personal medical information and sets out a cause of action for damages for patients whose individually identifiable medical information has been improperly released. Cal. Civ. Code § 56.101(a); *Sutter Health*, 227 Cal. App. 4th at 1551, 174 Cal. Rptr. 3d at 656. Under the CMIA, health care entities such as Premera are obligated not only to refrain from unauthorized disclosure of protected information, but to maintain such information "in a manner that preserves the confidentiality of the information contained therein." Cal Civ. Code § 56.101(a). Here, Plaintiff Hansen-Bosse seeks to certify a class of California policyholders. These class members have a

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

clear connection to California, and clear entitlement to the additional statutory protections of California's CMIA. Accordingly, this proposed Class does not raise any choice of law concerns.

Plaintiff Hansen-Bosse originally filed her action in the District of Oregon; consequently, Oregon's choice of law rules apply. *See In re United Parcel Serv.*, 580 F. App'x at 544. Because Oregon has no statute comparable to the CMIA, there is a material difference between the law of Oregon, the forum state where Hansen-Bosse originally filed suit, and the law of California. *See Bispo v. GSW Inc.*, No. 05–CV–1223–PK, 2007 WL 2034355, at *3 (D. Or. July 9, 2007) (for choice of law purposes, no actual conflict where there is no material difference in the laws of the two states).

Under the "most significant relationship" test set forth in Restatement § 145, Oregon has no significant relationship to the occurrence and the parties at issue. While Premera's conduct was centered in Washington, California has a significant relationship to the dispute with respect to the legal protections California established under the CMIA. Premera agreed to participate in the Blue Program and knowingly insured individuals who resided in California; it was therefore aware that it could be subject to additional statutory requirements in states where it provides insurance benefits.

Premera insured California residents such as Plaintiff Hansen-Bosse, and Premera's failure to comply with the statutory requirements of California results in the most significant relationship with California for this particular claim. This is true even if its general conduct that resulted in the statutory violation had the most significant relationship to Washington. Indeed, under the most relevant factor enumerated in § 6(2)(c) of the Restatement—"the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue"—California has a clear interest in ensuring that its citizens are protected by the

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

provisions of the CMIA. Neither Washington nor Oregon has a comparable statute of its own that would apply, and neither state has an interest in the additional application of a California statute to a class of California residents. Further, classwide application of the CMIA supports the purpose of the statute, which was enacted by the California legislature to "protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider, while at the same time setting forth limited circumstances in which the release of such information to specified entities is permissible." *Brown v. Mortensen*, 253 P.3d 522, 533 (Cal. 2011) (internal citations omitted). Given California's interest in the determination of Plaintiff Hansen-Bosse's CMIA claim and affording California residents the protections under this statute, this Court should apply California law to the CMIA Class's claim.

b. Other common issues of law and fact predominate for the CMIA Class.

Premera's negligence in failing to implement and maintain adequate information security protocols affected all members of the proposed CMIA Class in materially the same way. For each of the proposed CMIA Class members, Premera had in its system individually identifiable information relating to their medical history, condition, or treatment. Ex. 74 (Seymour Depo 2) at 42:8-16 (FACETS and other databases contain Sensitive Information); *see also, e.g.*, Ex. 65 at RFP 267; Strebe Decl. at ¶ 207. And the privacy of all of the medical information of the members of the proposed CMIA Class was compromised in the same way during the breach of Premera's system. Indeed, such a claim under the CMIA resulting from a data breach has been certified as a class action. Order Granting Plaintiffs' Motion for Class Certification, *St. Joseph Health Sys. Med. Info. Cases*, JCCP No. 4716 (Cal. Super. Ct., Orange Cnty. Dec. 5, 2014) (certifying CMIA class compromised of all individuals whose data was made accessible by a data breach of health care provider). Dubanevich Decl., Ex. 4. Further, the CMIA claim raises no

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

questions of individualized damages—if Premera is liable under the CMIA, the CMIA Class is entitled to nominal/statutory damages of $1000 per disclosure. Cal. Civ. Code § 56.36(b). These common issues of law and fact predominate any individual issues that might exist.

iv. Class adjudication is superior to other available methods.

In order to determine whether "a class action is superior to other available methods for fairly and efficiently adjudicating the controversy," Fed. R. Civ. P. 23(b)(3), a court may consider: (1) the class members' interests in individually controlling the prosecution of separate actions; (2) the extent of other litigation concerning the controversy; (3) the desirability of concentrating the claims in the particular forum; and (4) the likely difficulties in managing the class action. Fed. R. Civ. P. 23(b)(3)(A)-(D).

"[T]he purpose of the superiority requirement is to assure that the class action is the most efficient and effective means of resolving the controversy . . . ." 7AA Charles Wright, Arthur Miller & Mary Kay Kane, Federal Practice and Procedure, § 1779 (3d ed. 2005); *Wolin v. Jaguar Land Rover N. Am., LLC*, 617 F.3d 1168, 1175 (9th Cir. 2010). "Rule 23(b)(3)'s superiority test requires the court to determine whether maintenance of this litigation as a class action is efficient and whether it is fair. This analysis is related to the commonality test. Underlying both tests is a concern for judicial economy." *Id.* at 1175-76.

"'Where damages suffered by each putative class member are not large,' the first factor 'weighs in favor of certifying a class action.'" *Agne v. Papa John's Int'l, Inc.*, 286 F.R.D. 559, 571 (W.D. Wash. 2012) (quoting *Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1190 (9th Cir. 2001)). "The policy 'at the very core of the class action mechanism is to overcome the problem that small recoveries do not provide the incentive' for individuals to bring claims." *Id.* (quoting *Amchem*, 521 U.S. at 617). Courts have held the superiority requirement was met even

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

where the amount of damages could reach $1,500 per individual. *Kavu, Inc. v. Omnipak Corp.*, 246 F.R.D. 642, 650 (W.D. Wash. 2007); *see Rodriguez v. Experian Info. Solutions, Inc.*, No. C15-01224-RAJ, 2018 WL 1014606, at *6 (W.D. Wash. Feb. 22, 2018) (superiority requirement met where "relatively small" statutory damages of $1000 per violation under the Fair Credit Reporting Act would deter individual litigants). Where individual damages are small, "class members would be unlikely to litigate claims on their own," and the defendant would "avoid damages for the vast majority of its violations." *Kavu*, 246 F.R.D. at 650.

Like other proposed class actions, this case involves millions of individual class members, each of whom have suffered a relatively small amount of damages. Even at the high end of the estimates for recovery, individual litigation would be cost-prohibitive.[25] *See Chamberlan v. Ford Motor Co.*, 402 F.3d 952, 960 (9th Cir. 2005) ("[T]he district court did not abuse its discretion in finding that, absent a class action, Class Plaintiffs would have no meaningful redress against Ford."). Here, litigating through a class action is superior to leaving Plaintiffs and the proposed class members without a viable means of pursuing their claims.

Concentrating the litigation in a single forum is desirable. Resolving these claims in a single action will avoid the potential for inconsistent results, will decrease the expenses of litigation, and will promote judicial economy. And because Plaintiffs will prove their case with classwide evidence, it is desirable to litigate and resolve these claims in a single forum. As the court said in *Wolin*:

> Proposed class members face the option of participating in this class action, or filing hundreds of individual lawsuits that could involve duplicating discovery and costs that exceed the extent of proposed class members' individual injuries.

[25] With Premera's denial of wrongdoing, individual plaintiffs in individual lawsuits would be required to spend millions on discovery alone.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

> Thus, classwide adjudication of appellants' claims is superior to other means of adjudicating this case.

Wolin, 617 F.3d at 1176.

Finally, class treatment of this action is manageable. The proposed classes are comprised of well-defined groups of individuals, easily identified from Premera's records. Because Premera's liability will be determined by common evidence of Premera's statements regarding data security and Premera's IT policies and procedures, a class trial would be easily managed. Plaintiffs will rely at trial on binding admissions, discovery responses, and 30(b)(6) deposition testimony, in addition to common evidence regarding Premera's policies and testimony regarding its security practices. For all of these reasons, a class action is a superior method for fairly and efficiently adjudicating the claims of the members of the proposed classes.

v. Certification of issues under Rule 23(c)(4) is also appropriate.

Should the Court determine the individualized issues of causation or damages for certain of class members' injuries overwhelms common questions, Plaintiffs request that the Court certify the common issues of: 1) Whether Premera's Notices of Privacy Practices constituted a contract with members; 2) Whether Premera breached that contract; 3) Whether Premera had a duty protect class members' Sensitive Information; and 4) Whether Premera breached that duty. The resolution of these common questions would significantly advance the litigation and allow for follow on mini-trials by individual plaintiffs seeking damages.

"When appropriate," Rule 23(c)(4) allows a court great discretion to certify an action "as a class action with respect to particular issues." Fed. R. Civ. P. 23(c)(4). It does not prescribe elements that representatives must show in order to maintain an issue class, but courts recognize its value in resolving cases where denying certification of common issues would all but strip class members of their right to seek relief. The Ninth Circuit has endorsed the use of issue

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

certification. *Valentino*, 97 F.3d at 1233-34. Many other circuit courts have, as well. *See In re Deepwater Horizon*, 739 F.3d 790, 817 (5th Cir. 2014); *Butler v. Sears, Roebuck & Co.*, 727 F.3d 796, 800-02 (7th Cir. 2013); *In re Whirlpool Corp. Front-Loading Washer Prods. Liab. Litig.*, 722 F.3d 838, 860-61 (6th Cir. 2013); *see also Jimenez v. Allstate Ins. Co.*, 765 F.3d 1161, 1168 (9th Cir. 2014) (noting *Butler*, *Whirlpool*, and *Deepwater Horizon* "are compelling . . . [a]nd their reasoning is consistent with our circuit precedent").

Basic liability questions predominate for Plaintiffs' contract, negligence, CPA, and CMIA claims. If the Court determines that class members' lost value of PII or losses from identity theft require a more specific showing of causation, and defeat predominance, it may still allow Plaintiffs to proceed under Rule 23(c)(4). *Tasion Commc'ns, Inc. v. Ubiquiti Networks, Inc.*, 308 F.R.D. 630, 633 (N.D. Cal. 2015) (Rule 23(c)(4) issues class "must still meet the requirements of Rule 23(a) and (b) (except for the predominance requirement of Rule 23(b)(3))"). The Court may certify issues under Rule 23(c)(4) if it materially advances the litigation as a whole, with the focus being "judicial economy and efficiency." *Kamakahi v. Am. Soc'y for Reprod. Med.*, 305 F.R.D. 164, 193 (N.D. Cal. 2015) (internal citation omitted).

C. Plaintiffs' Injunctive Relief Class Satisfies the Elements of Rule 23(b)(2)

Members of the proposed Injunctive Relief class are a subset of the CPA Class whose data was on Premera's system on March 6, 2015 and whose data remains within Premera's databases. In addition to injunctive relief sought by the CPA Class for ongoing fraud-detection services, the Injunctive Relief Class additionally seeks final injunctive relief to require Premera to remediate outstanding issues that leave their Sensitive Information at risk for further exposure.

Class certification of a claim for injunctive relief is appropriate when, in addition to the four requirements of 23(a) discussed above, "the party opposing the class has acted or refused to

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

act on grounds that apply generally to the class, so that final injunctive relief . . . is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). Here, members of the Injunctive Relief Class easily meet that standard because Premera acted in a manner common to the class in both failing to adequately protect the Sensitive Information within its possession and in failing to adequately remediate its systems to ensure that such information is not at continued risk of exposure.

Premera stored all class members' data in the same databases, with the same deficient security, and class members' Sensitive Information was compromised as a result of those deficiencies. Premera is still in possession of class members' Sensitive Information, and has still not taken all reasonably necessary measures to secure it adequately. The measures that Premera took to secure Plaintiffs' Sensitive Information since the breach, and the additional measures still required will be established by common evidence of Premera's actions and inactions as well as through expert testimony. Because Premera's actions pose a continuing threat to the security of Plaintiffs' and the class members' Sensitive Information, final injunctive relief is necessary to order Premera to remediate its poor security, and will be the same for all class members. *See, e.g.*, *Delarosa v. Boiron, Inc.*, 275 F.R.D. 582, 591-92 (C.D. Cal. 2011); *Jermyn v. Best Buy Stores, L.P.*, 256 F.R.D. 418, 434 (S.D.N.Y. 2009).

Plaintiffs likewise seek to require Premera to provide the class members with appropriate fraud-prevention, detection services, and insurance services to mitigate the deleterious effects of its prior sub-standard security practices.[26] *See Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-

[26] To the extent the Court is inclined to view the cost to maintain credit monitoring as damages, the cost is uniform per person and can be calculated on a classwide basis. Wolfson Damages Decl., Ex. 1.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

09600 RGK (Ex), 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015) (credit monitoring is necessary for victims of data breach).

Defendants' failure to provide adequate data security applies to everyone in these classes, necessitating the same remedy for all class members. Thus, "a single injunction . . . would provide relief to each member of the class." *Wal-Mart*, 564 U.S. at 360; *Rodriguez v. Hayes*, 591 F.3d 1105, 1125 (9th Cir. 2010) (court need "only to look at whether class members seek uniform relief from practice applicable to all of them"); *Parsons v. Ryan*, 754 F.3d 657, 688-89 (9th Cir. 2014) ("[B]y allegedly establishing systemic policies and practices . . . the defendants have acted on grounds that apply generally to the proposed class and subclass, rendering certification under Rule 23(b)(2) appropriate.").

V. CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that this Court grant their motion and certify the proposed classes, or in the alternative, certify such classes on issues as it determines is just and appropriate. Plaintiffs further request that this Court appoint Kim D. Stephens of Tousley Brain Stephens LLC as Class Counsel; Keith Dubanevich of Stoll Berne as Liaison Counsel; James Pizzirusso of Hausfeld LLP, Tina Wolfson of Ahdoot & Wolfson, and Karen Hanson Riebel of Lockridge Grindal & Nauen PLLP to the Executive Committee; and Plaintiffs April Allred, Elizabeth Black, Ralph Christopherson, Barbara Lynch, Sharif Ailey, Catherine Bushman, Krishnendu Chakraborty, Maduchdanda Chakraborty, Eric Forseter, Mary Fuerst, Ross Imbler, Kevin Smith, and Debbie Hansen-Bosse as class representatives.

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 S.W. OAK STREET, SUITE 500
PORTLAND, OREGON 97204
TEL. (503) 227-1600 FAX (503) 227-6840

DATED: August 3, 2018

TOUSLEY BRAIN STEPHENS PLLC

/s/ Kim D. Stephens

Kim D. Stephens, OSB No. 030635
Christopher I. Brain, *admitted pro hac vice*
Jason T. Dennett, *admitted pro hac vice*
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
Email: kstephens@tousley.com
cbrain@tousley.com
jdennett@tousley.com

Interim Lead Plaintiffs' Counsel

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.

/s/ Keith S. Dubanevich

Keith S. Dubanevich, OSB No. 975200
Yoona Park, OSB No. 077095
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840
Email: kdubanevich@stollberne.com
ypark@stollberne.com

Interim Liaison Plaintiffs' Counsel

Tina Wolfson
AHDOOT AND WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069
Tel: (310) 474-9111
Fax: (310) 474-8585
Email: twolfson@ahdootwolfson.com

James Pizzirusso
HAUSFELD LLP
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: (202) 540-7200
Fax: (202) 540-7201
Email: jpizzirusso@hausfeldllp.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
Email: khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Plaintiffs' Executive Leadership Committee